Titre: Title:	Analyse du risque en matière de cybersécurité de l'écosystème des dispositifs électroniques cardiaques implantables (DECI)
Auteur: Author:	Mikaela Stéphanie Ngamboe Mvogo
Date:	2019
Type:	Mémoire ou thèse / Dissertation or Thesis
Référence: Citation:	Ngamboe Mvogo, M. S. (2019). Analyse du risque en matière de cybersécurité de l'écosystème des dispositifs électroniques cardiaques implantables (DECI) [Mémoire de maîtrise, Polytechnique Montréal]. PolyPublie. https://publications.polymtl.ca/3877/

URL de PolyPublie: PolyPublie URL:	https://publications.polymtl.ca/3877/
Directeurs de recherche: Advisors:	Katia Dyrda, & Jose Manuel Fernandez
Programme: Program:	Génie informatique

UNIVERSITÉ DE MONTRÉAL

ANALYSE DU RISQUE EN MATIÈRE DE CYBERSÉCURITÉ DE L'ÉCOSYSTÈME DES DISPOSITIFS ÉLECTRONIQUES CARDIAQUES IMPLANTABLES (DECI)

MIKAELA STÉPHANIE NGAMBOE MVOGO
DÉPARTEMENT DE GÉNIE INFORMATIQUE ET GÉNIE LOGICIEL
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

MÉMOIRE PRÉSENTÉ EN VUE DE L'OBTENTION
DU DIPLÔME DE MAÎTRISE ÈS SCIENCES APPLIQUÉES
(GÉNIE INFORMATIQUE)
MAI 2019

UNIVERSITÉ DE MONTRÉAL

ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Ce mémoire intitulé :

ANALYSE DU RISQUE EN MATIÈRE DE CYBERSÉCURITÉ DE L'ÉCOSYSTÈME DES DISPOSITIFS ÉLECTRONIQUES CARDIAQUES IMPLANTABLES (DECI)

présenté par : NGAMBOE MVOGO Mikaela Stéphanie
en vue de l'obtention du diplôme de : Maîtrise ès sciences appliquées
a été dûment accepté par le jury d'examen constitué de :

Mme CHERIET Farida, Ph. D., présidente
M. FERNANDEZ José M., Ph. D., membre et directeur de recherche
Mme DYRDA Katia, MD, membre et codirectrice de recherche
Mme NICOLESCU Gabriela, Doctorat, membre

DÉDICACE

J'ai placé ma confiance dans la mer de ta miséricorde,
et mes espoirs n'ont pas été déçus. J'ai confiance en TOI...

En el mar de tu misericordia deposité mi confianza,
y mis esperanzas no fueron defraudadas. Confío en TI...

REMERCIEMENTS

À Dieu par qui je fais tout et à qui je dois tout.
À la Sainte Vierge Marie et à Saint Joseph à qui j'ai consacré mes études.

À mes chers parents, vous êtes mon modèle et mon réconfort. Merci papa et maman pour votre amour inconditionnel et pour toutes les valeurs que vous m'avez inculqués.
À mes frères Jean-Marc, Willy et José Maria, vous êtes ma joie et ma fierté.
À mes belles sœurs Nati et Leti ainsi que mes neveux Léo et Iwa, votre arrivée dans la famille est une bénédiction.

À mon directeur de recherche M. José Manuel Fernandez, merci pour toutes les opportunités que tu m'as données. Merci aussi pour ton humanité et ta générosité.
À ma codirectrice Mme Katia Dyrda, merci d'avoir accepté de me codiriger, de m'avoir fourni les équipements nécessaires pour réaliser ce projet. Merci pour tes paroles de soutien.
Aux attachés de recherche du SecSI Militza, Paul, Nader et Ranwa, pour vos conseils, corrections et amitié.
À tous mes camarades du SecSI, vous avez ensoleillé mes jours de travail.

Aux frères Réal et René merci pour votre accueil et bienveillance envers moi. En vivant avec vous, j'ai appris ce qui veut dire le don de soi.
Finalement, mais pas moins important, à la "Team de Willowdale", tous mes colloques depuis le mois d'août 2015 et Doudoune. Merci pour les grands moments passés ensemble.

RÉSUMÉ

L'utilisation des dispositifs électroniques cardiaques implantables (DECI) équipés de fonctionnalités de télémétrie augmente en raison des avantages qu'ils apportent à la qualité des soins aux patients, au rendement du personnel médical et à la réduction des coûts en santé. Ils interagissent avec des systèmes externes situés à l'hôpital (programmeur), au domicile des patients (moniteur à domicile) et dans le nuage. Les DECI communiquent avec les programmeurs et les moniteurs domestiques par l'intermédiaire de signaux radiofréquence (RF) transmis dans la bande des services de communication pour implants médicaux (MICS 402-405 Mhz), tandis qu'ils interagissent avec les systèmes en nuage par l'intermédiaire des moniteurs domestiques et de la connectivité IP (protocole Internet). Les DECI sont vulnérables aux cyberattaques qui exploitent leur interface de communication par radiofréquence. Cela vaut également pour les DECI non équipés de télémétrie, mais la télémétrie introduit des vecteurs d'attaque supplémentaires. La mise en garde de la *Food and Drug Administration* (FDA) concernant près d'un demi-million de DECI en 2017, selon laquelle ces dispositifs étaient vulnérables à un accès non autorisé, permettant à une personne malveillante de les reprogrammer à l'aide d'équipements disponibles sur le marché, témoigne de la croissante inquiétude que suscitent les cyberattaques contre les DECI. Bien que les DECI puissent être vulnérables, aucune cyberattaque de ce type n'a été signalée. Bien que nous sachions qu'il est techniquement possible de mener de telles attaques dans l'environnement contrôlé d'un laboratoire de recherche, il reste à déterminer dans quelle mesure de telles attaques seraient viables sur une cible réelle dans le monde réel. Nous avons cherché à évaluer les risques réels des cyberattaques contre les DECI équipés de télémétrie et des systèmes dont ils dépendent. Nous avons effectué une analyse de risque réaliste de ces attaques. Un inventaire des vulnérabilités qui ont été rendues publiques à ce jour a été réalisé. Des scénarios d'attaque ont été déterminés sur la base de ces vulnérabilités, en évaluant pourquoi et comment un cybercriminel pourrait les exploiter à des fins malveillantes. La probabilité d'une exploitation malveillante de chaque vulnérabilité a été estimée en fonction de trois critères : la capacité, la motivation et l'opportunité des cybercriminels. Des cyberattaques ont été simulées dans notre laboratoire à l'aide de DECI et de programmeurs. Nous avons déterminé l'impact des cyberattaques selon quatre échelles distinctes : santé, économie, vie privée et qualité de vie. L'impact sur la santé a été déterminé selon la classification Hayes des interférences cliniquement significatives avec les fonctions des DECI, tandis que le reste des impacts ont été déterminés selon le *Fair Information Practice Principles* 999 (FIPPS), un standard pour l'évaluation de sécurité des systèmes de l'information. Enfin, le risque associé à chaque

vecteur d'attaque a été calculé en multipliant sa probabilité d'exploitation par son impact. Deux des six objectifs d'attaque possibles représentent un risque critique , à savoir "Inciter le personnel médical à commettre des erreurs de diagnostic" et "Acquérir des connaissances sur le fonctionnement de l'appareil et des logiciels". Quatre des 15 vulnérabilités identifiées représentent un risque inacceptable, toutes associées à des dispositifs externes (programmeur et moniteur à domicile) et sont exploitables via l'accès réseau ou l'accès web aux cibles. Les résultats de cette étude révèlent que les menaces associées à l'interface de communication RF des DECI représentent un risque acceptable par rapport à la connectivité IP des appareils externes (programmateur et moniteur domestique). Le risque réel se trouve dans les réseaux informatiques et dans le nuage. Il existe plusieurs solutions à ce problème. Il est donc à la portée des groupes affectés (patients, personnel de santé, fabricants et autorités gouvernementales) de prendre les mesures nécessaires pour réduire les risques associés à de telles cyberattaques.

ABSTRACT

The use of telemetry-enabled Cardiac Implantable Electronic Devices (CIED) is increasing due to the significant advantages it brings to patient care quality, medical staff performance and reductions in health cost. They interact with external systems located in the hospital (programmer), in patient homes (home monitor) and in the cloud. CIED communicate with programmers and the home monitors via Radio Frequency (RF) signals transmitted in the Medical Implants Communication Services band (MICS 402-405 Mhz), whereas they interact with cloud-based systems via home monitoring devices and Internet Protocol (IP) connectivity. CIED are vulnerable to cyber attacks that use their Radio Frequency communication interface. This also holds for non-telemetry enabled CIED, but telemetry capability introduces additional vectors of cyber attacks. The increased concern of cyber attacks on telemetry-enabled CIED was demonstrated by the Food and Drug Administration (FDA) warning affecting almost half a million CIED in 2017 stating the aforementioned devices were vulnerable to unauthorized access, allowing a malicious person to reprogram them using commercially available equipment. Although CIED may be vulnerable, no such cyber attacks have been reported. While we know it is technically possible to conduct such an attack in the controlled environment of a research laboratory, it remains to be determined how viable such an attack would be on an actual target in the real world. We sought to assess the real-life risks of cyber attack on telemetry enabled CIED and the systems they depend on. We carried out a realistic risk analysis of such attacks. An inventory of the vulnerabilities that have been made public to date was performed. Attack scenarios were determined based on those vulnerabilities, assessing why and how a cybercriminal could exploit them for malicious purpose. The likelihood of malicious exploitation of each vulnerability was estimated according to three criteria: cybercriminal ability, motivation, and opportunity. Cyber attacks were emulated in our laboratory using current CIED and programmers. We determined the impact of cyberattacks according to four separate scales: health, economy, privacy and quality of life. The impact on health was determined according to the Hayes classification of clinically significant interference with CIED function while the rest of impacts was determined with the Fair Information Practice Principles 999 (FIPPS), a standard for the security assessment of information systems. Finally, the risk associated with each attack vector was computed by multiplying its exploitation likelihood by its impact. Two of the six possible attack goals represent a critical risk namely “Induce medical staff to make diagnostic errors” and “Gain knowledge of device operation and software”. Four of the 15 inventoried vulnerabilities represent a critical risk; all associated to external devices (programmer and

home monitor) and exploited by network access and web acess. The risk of exploiting CIED RF communication interface is minor compared to the risk of exploiting externals devices IP connectivity. The real risk lies in computer networks, and there are several solutions. It is therefore within the reach of affected groups (patients, health personnel, manufacturers and government autorities) to take necessary measures to reduce the risks associated to such cyberattacks.

TABLE DES MATIÈRES

LISTE DES TABLEAUX

LISTE DES FIGURES

LISTE DES SIGLES ET ABRÉVIATIONS

CIED	Cardiac Implantable Electronic Devices
CMOS	Complementary Metal-Oxide Semiconductor
DECI	Dispositifs électroniques cardiaques implantables
DHS	Departement of Homeland Security
DoS	Denial of Service
FCC	Federal Communications Commission
FDA	Food and Drug Administration
FIPPS	Fair Information Practice Principles
HIS	Health Infrastructure Systems
HIPPA	Health Insurance Privacy and Portability Act
IAM	Identity and Access Management
IC	Integrated Circuit
ICS-CERT	Industrial Control System Computer Emergency Response Team
ICT	Information and Communications Technologies
IMD	Implantable Medical Devices
ISS	Infrastructures des systèmes de santé
ITSEC	Information Technology Security Evaluation Criteria
ITU-R	International Telecommunications Union - Radio communication
JTAG	Joint Test Action Group
MITM	Man in the Middle
NIST	National Institute of Standards and Technology
OS	Operating System
RDS	Radio définie par software
RF	Radio fréquence
SDR	Software Defined Radio
STRIDE	Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege
USB	Universal Serial Bus
UART	Universal Asynchronous Receiver Transmitter
VPN	Virtual Private Network

LISTE DES ANNEXES

CHAPITRE 1 INTRODUCTION

La médecine a toujours exploré et profité des avancées technologiques pour améliorer la santé des patients. Les dispositifs électroniques cardiaques implantables (DECI) en sont un exemple. Ces appareils sont prescrits pour traiter les troubles du rythme cardiaque [1], d'après la *World Society of Arrhythmias* plus de 1 002 664 DECI sont actuellement implantés dans 61 pays parmi lesquels les É.U et le Canada [2]. On prévoit que d'ici 2023 le nombre d'unités implantés dans le monde atteindra 1,4 million [3]. Les DECI sont les dispositifs médicaux ayant évolué avec le plus de célérité au cours des deux derniers siècles [4]. Depuis leur apparition à la fin des années 1950, leurs performances cliniques n'ont fait que s'accroître. En effet, certains des modèles actuels ont un temps de service de plus de 10 ans [1], plusieurs applications cliniques et possèdent des fonctionnalités de plus en plus sophistiquées [5, 6].

Cet accroissement de performance résulte du travail en équipe des compagnies de fabrication de stimulateurs cardiaques et des laboratoires de recherche médicale. Ils ont su mettre à profit les avancées technologiques arrivant dans plusieurs disciplines (batterie, micro-électronique, informatique) pour concevoir des DECI plus sécuritaires du point de vue clinique [4]. De ce travail en commun a résulté une amélioration de la qualité de vie des patients, des conditions de travail du personnel médical et une réduction des coûts associés à la santé [6].

Cependant, l'effort mis pour améliorer les performances cliniques des DECI, n'a pas été le même que celui mis pour tester la sécurité informatique des fonctionnalités responsables de cette hausse de performance. Par conséquent, les DECI modernes sont vulnérables aux attaques informatiques [7–14]. En sont la preuve les vulnérabilités dévoilées dans certains travaux de recherche [7–9], des preuves de concept d'attaques [10, 13] ou plus récemment, le rappel de près de 500 000 DECI effectué aux É.U au mois d'août 2017 par la *Food and Drug Aministration* (FDA) [11].

1.1 Mise en contexte sur les DECI

Les DECI sont des équipements médicaux prescrits pour traiter les troubles du rythme cardiaque. Ils se composent d'une sonde et d'un générateur d'impulsions électriques [1, 15].

La sonde est un fil de conduction électrique qui relie le stimulateur cardiaque au coeur (Figure 1.1 [16]). De façon générale, elle s'insère par la veine sous-clavière, axillaire ou céphalique. Elle est par la suite fixée a une paroi du coeur par le moyen de électrode hélicoïdale présent dans une de ses extrémités. La sonde cardiaque assure deux fonctions. D'une part, elle détecte

l'activité électrique de l'organe. D'autre part, elle lui achemine les signaux issus du générateur d'impulsions électriques [1, 4].

Le générateur d'impulsions électrique (Figure 1.2 [15]) se compose d'une pile en lithium-iode et d'un circuit électrique.

La pile alimente le circuit électrique afin qu'il produise les impulsions nécessaires pour stimuler le cœur. Son temps de service est en moyenne de 10 ans (Cardiostimulateur). L'épuisement de la pile rend le DECI inutilisable [15,17]. De ce fait, avant qu'une pareille situation n'advienne, le patient est soumis a une opération chirurgicale pour se faire explanter son DECI puis implanter un nouveau dispositif.

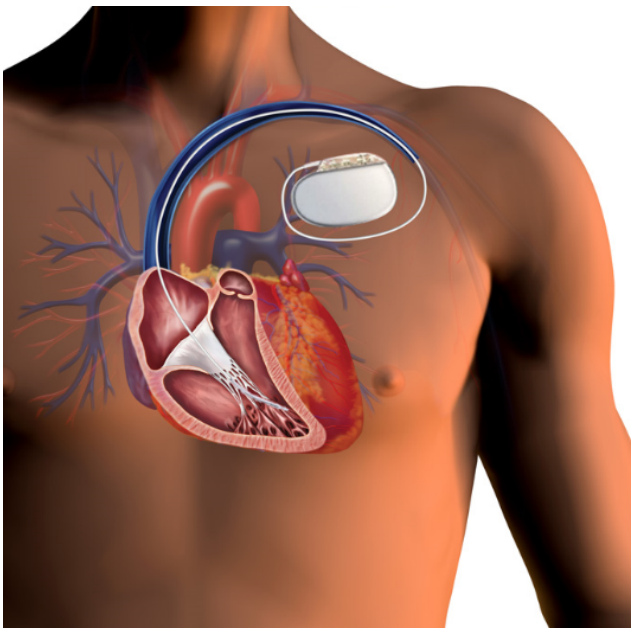

Figure 1.1 DECI implanté dans la région pectorale (source [16])

Les circuits électriques des DECI modernes se composent de plusieurs circuits intégrés. Notamment, un microprocesseur, deux mémoires (ROM et RAM), une horloge de synchronisation, un block de télémétrie, etc. [6, 18–22]. Le microprocesseur interprète les signaux cardiaques provenant de la sonde de détection et donne des instructions au reste des éléments de la circuiterie afin que le DECI fasse ce qu'il est sensé faire en tout moment. La mémoire ROM stocke le firmware du dispositif tandis que la RAM stocke le code de la thérapie à appliquer au patient et les paramètres de son activité cardiaque. L'horloge synchronise la stimulation des oreillettes et des ventricules. En dernier lieu, le bloc de télémétrie établit une communication sans fil entre le DECI et deux types de dispositifs externes.

Les DECI communiquent via des signaux RF avec les programmeurs externes des hôpitaux et les moniteurs logés au domiciles des patients. Cette communication a lieu dans la bande de fréquence du MICS : celle ci va de 402 à 405 Mhz [23]. Le programmeur externe est employé par le personnel médical lors des visites cliniques. Il sert à la fois à lire les paramètres d'activité cardiaque du patient, à programmer le DECI selon les besoins du patient et à tester le mode de fonctionnement du dispositif [24, 25]. Le moniteur au domicile récolte périodiquement les paramètres de l'activité cardiaque du patient puis les envoie à une base de données logée dans le nuage. Ainsi, lorsqu'un cardiologue souhaite voir le relevé de l'activité cardiaque de son patient, il accède au contenu de la base de données par une application web développée par le fabricant des DECI ou par un distributeur de services web embauché à cet effet [26–28].

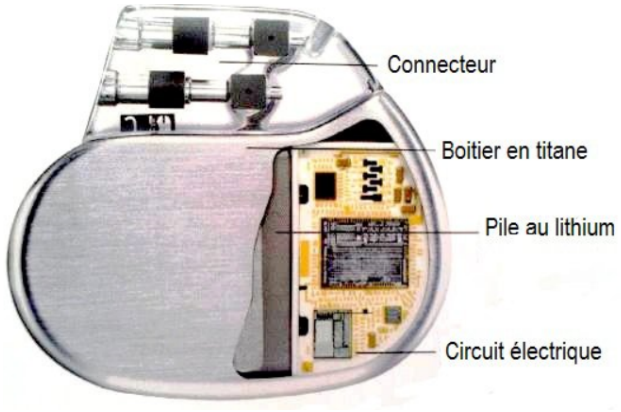

Figure 1.2 Composition des DECI (source [15])

1.2 Évolution des DECI en termes de performance

Depuis leur apparition a la fin des années 1958, les DECI connaissent une évolution en continue. En effet, ce sont les dispositifs médicaux dont la performance clinique a évolué avec le plus de célérité [29].

L'emploi de piles en lithium-iode comme source d'alimentation du générateur d'impulsions électriques en est une des raisons. Ces piles sont devenues la source d'alimentation standard des DECI du fait qu'elles offrent de meilleures caractéristiques sur le plan de la durabilité et de la fiabilité par rapport à leurs prédécesseurs. Nous pensons notamment aux piles au nickel/cadmium, celles rechargeables à travers la peau par signaux RF (radiofréquence), celles au zinc-mercure, les piézoélectriques, les biogalvaniques et les nucléaires [30, 31]. Les piles en lithium-iode se caractérisent principalement par leur densité d'énergie élevée et leur faible

taux d'auto-décharge [17,32,33]. Ces caractéristiques ont contribué à élargir le temps de service des DECI. Actuellement, ce temps est d'une durée de 10 ans environ. Par conséquent, les conditions de vie des patients ont connu une amélioration. En effet, chaque fois que la pile du DECI est sur le point de s'épuiser, les patients doivent subir une opération chirurgicale pour le remplacement de leur dispositif. Avec l'emploi des piles en lithium-iode, la fréquence de ces opérations a considérablement diminué. Par ailleurs, les applications cliniques des dispositifs en étude n'ont fait que s'élargir au cours des années, augmentant ainsi leur performance du point de vue médical. Assurément, les premiers DECI étaient des stimulateurs cardiaques à fréquence fixe, capables de traiter une pathologie nommée syndrome d'Adams-Stokes [6] . Cependant, les DECI actuels sont en mesure de traiter tout un éventail de pathologies cardiovasculaires du fait qu'ils possèdent à la fois les fonctionnalités de défibrillateur, de stimulateur cardiaque et de dispositif de resynchronisation cardiaque [4]. Cette multifonctionnalité est due à l'insertion de circuits intégrés dans leur circuiterie. Notamment, un microprocesseur, des mémoires, des registres, une horloge de synchronisation et des modules de communication. Par conséquent, la circuiterie des DECI modernes suit l'architecture informatique générale où les fonctions (opérations) à effectuer par le dispositif sont spécifiées par logiciel. Les stimulateurs cardiaques modernes sont donc programmables par logiciel, avant et après l'implantation du dispositif [6, 18–23, 34]. Leur mode de fonctionnement est configuré selon les besoins particuliers du patient. En résulte ainsi une amélioration de la qualité de leurs soins, de leurs conditions de santé et de leur qualité de vie.

L'insertion des fonctionnalités de télémétrie s'est avérée un facteur de performance décisif pour les raisons qui suivent. D'une part, la programmation des DECI se fait par télémétrie en employant un dispositif nommé programmeur externe [24, 25], qui communique par signaux RF avec les DECI pour accomplir le suivi, le diagnostic et le réglage de la thérapie du patient. Il opère selon trois modes de fonctionnement : 1) le *mode interrogation* afin d'extraire les paramètres d'activité cardiaque du patient ; 2) le *mode test* pour vérifier que le stimulateur cardiaque fonctionne adéquatement ; 3) le *mode programmation* pour configurer le mode de fonctionnement du dispositif. D'autre part, la télémétrie a favorisé le suivi à distance du patient. Il est devenu pratique courante de fournir aux patients un dispositif nommé *moniteur* [26–28]. Ce dernier collecte périodiquement les paramètres cardiaques du patient puis les envoie à une base de données logée dans le nuage. Ainsi, les médecins peuvent accéder à tout moment et en tout lieu au dossier médical des patients à travers une application web pouvant appartenir au fabricant des DECI ou à un fournisseur de service web. Hormis l'affichage quotidien des paramètres cardiaques du patient, ces applications émettent des alarmes lorsque son état de santé s'aggrave. L'on peut ainsi dire que l'insertion des fonctionnalités de télémétrie a contribué à améliorer la qualité de vie du patient du fait qu'avec le moniteur, le

nombre de visites à l'hôpital peut être réduit jusqu'à une seule par année, à diminuer les coûts associés à la santé, et à améliorer les conditions de travail du personnel médical [4, 24–28].

1.3 Éléments de la problématique

Les DECI modernes sont dotés de fonctionnalités qui les rendent accessibles et manipulables par des tiers à distance. Cependant, l'insertion desdites fonctionnalités a eu lieu en priorisant la sécurité clinique des dispositifs au détriment de leur sécurité informatique. Par conséquent, les DECI modernes ainsi que les systèmes avec lesquels ils interagissent sont vulnérables aux attaques informatiques. Les mesures de sécurité adoptées par les éléments de l'écosystème en étude ne sont pas suffisamment robustes. Cette situation est due, d'une part, aux contraintes en termes de ressources que présentent les stimulateurs cardiaques implantables, et d'autre part, au phénomène « d'insécurité par obscurité » régnant aux alentours des DECI. En effet, il existe une surabondance d'information concernant les vulnérabilités informatiques dont ils font l'objet [35–40]. Cependant, cette information n'est aucunement accompagnée de : 1) l'impact clinique et technologique réel qu'aurait l'exploitation malveillante desdites vulnérabilités et 2) le scénario d'attaque dans lequel elles pourraient être exploitées, i.e. où, quand et comment l'exploitation aurait lieu. Cette situation a créé une peur paralysante au sein des individus. Par conséquent, ils ne prennent pas les mesures de sécurité adéquates pour protéger l'accès à leur réseau ou dispositif, car ils pensent que la solution du problème n'est pas à leur portée.

1.3.1 Problèmes liés à l'interface de communication RF des DECI

L'interface de communication RF des DECI constitue un potentiel vecteur d'attaques informatiques contre les stimulateurs cardiaques [7,9,14]. Ce fait est d'autant plus vrai qu'au mois d'août 2017, la FDA a effectué le rappel volontaire d'environ un demi-million de DECI [11]. D'après cet organisme de réglementation américaine en matière de santé, ces dispositifs seraient vulnérables aux accès non autorisés achevés par le moyen de dispositifs grand marché, tels qu'une radio définie par logiciel (*Software-Defined Radio*, ou SDR). Ainsi, une personne malintentionnée serait en mesure d'exploiter l'interface de communication RF des DECI pour intercepter les données sensibles échangées entre le stimulateur cardiaque et les dispositifs externes avec lesquels il interagit, voire pire, le reprogrammer. Le rappel de la FDA [11] a corroboré ce que certains travaux antérieurs avaient mis en évidence dans le passé, à savoir que les mécanismes d'authentification des DECI sont faibles [7–9]. De nos jours, il existe maintes solutions pour pallier ce problème. Nous pensons notamment aux méthodes cryptographiques. Mais celles-ci ne sont pas directement applicables aux DECI en raison des contraintes de res-

sources qu'ils présentent. En effet, les stimulateurs cardiaques implantables sont limités en termes d'énergie, de capacité de stockage et de capacité computationnelle [41–43]. Un protocole d'authentification robuste nécessite l'exécution multiple d'au moins trois algorithmes. D'une part, un algorithme de chiffrement asymétrique et symétrique pour assurer l'authentification et la confidentialité. D'autre part, un haché de message pour garantir l'intégrité de l'information [41]. Or, de tels algorithmes peuvent exiger une capacité de calcul élevé, c'est-à-dire une grande quantité d'énergie qui pourrait épuiser la batterie des DECI plus tôt que prévu. Par ailleurs, un espace mémoire suffisant s'avérerait nécessaire pour stocker les paramètres secrets de la clé cryptographique [42] . Cependant, cet espace est restreint du fait que les mémoires des DECI doivent stocker plusieurs données à savoir, les codes de la thérapie à appliquer au patient ainsi que leurs paramètres cardiaques. Des méthodes alternatives d'authentification ont été proposées. Certaines solutions se basent sur les données biométriques des individus [44–46], d'autres sur la proximité entre dispositifs [47], et certaines proposent l'emploi d'un dispositif mandataire [48, 49]. Néanmoins, aucune d'elles ne semble satisfaire adéquatement le compromis devant se donner entre la sécurité technologique des dispositifs et leur sécurité clinique.

1.3.2 Problèmes liés aux fonctionnalités de télémétrie et connectivité IP des dispositifs externes

La télémétrie constitue un potentiel vecteur d'attaque contre les éléments de l'écosystème des DECI [8]. Ces systèmes sont accessibles par réseau (programmeur externe et serveur de base de données) ou accèdent au réseau (moniteur à la maison). Bien que les DECI en soi n'accèdent pas directement au réseau, la télémétrie s'avère aussi un vecteur d'attaque pour eux. Cela s'explique par le fait qu'ils interagissent d'une manière ou d'une autre avec des systèmes qui accèdent ou sont accessibles par réseau. Par conséquent, si les mesures de sécurité adéquates ne sont pas prises, une personne malveillante pourrait accomplir des attaques informatiques par le moyen des fonctionnalités de télémétrie qu'offrent les dispositifs externes de l'écosystème des DECI. L'attaquant pourrait alors exploiter les fonctionnalités de télémétrie du moniteur pour intercepter les données sensibles du patient, modifier ces données ou encore modifier les paramètres de fonctionnement du dispositif. L'exploitation malveillante des fonctionnalités de télémétrie du programmeur lui permettrait aussi d'accomplir de pareils objectifs d'attaque. En s'attaquant aux systèmes du nuage, l'adversaire pourrait non seulement avoir accès aux données sensibles de plusieurs individus, mais aussi les modifier ou, pire, interrompre l'accès à ces données.

1.4 Objectifs de recherche

Il existe de nos jours des « boîtes à outils » de contre-mesures pour éviter les cyberattaques contre les systèmes informatiques traditionnels, le chiffrement (symétrique ou asymétrique) ou le hachage cryptographique en sont certaines. Cependant, ces solutions ne peuvent être directement appliquées aux DECI en raison des contraintes de ressources qu'ils présentent [42, 48, 49]. De plus, bien que les dispositifs externes dont les DECI dépendent ne soient contraints en termes de ressources, les mesures de sécurité qui y sont implantées ne sont pas idéales. Ceci ce doit a une divulgation inadéquate des informations concernant les vulnérabilités dont ils font l'objet. D'une part, cette information est technique et grand nombre des parties affectées (patients et médecins) ne la comprennent pas [36–38, 40, 50–52]. D'autre part, cette information ne décrit pas les scénarios d'attaques (ou, quand et comment) où est ce que ces vulnérabilités pourraient être exploitées. Par conséquent, les parties concernées ne sont pas dans la mesure de se protéger adéquatement du fait que non seulement elle ne connaissent la portée du risque qu'elles encourent mais aussi parce qu'elle ne savent pas où se trouve exactement le risque. Afin de répondre à ce besoin, nous avons réalisé une analyse du risque en matière de cybersecurité des DECI et des systèmes externes dont ils dépendent. L'objectif général de ce travail de recherche est de déterminer le risque d'exploitation réel des vulnérabilités qui ont été dévoilées à ce jour dans l'écosystème des DECI. Dans cette ligne de pensée, la question de recherche suivante à été formulée :

> *Quel est le risque d'exploitation réel des vecteurs d'attaque (vulnérabilités) affectant l'écosystème des DECI ?*

Afin de donner réponse a cette question, nous nous sommes fixé trois objectifs spécifiques :

1. *Déterminer l'impact des attaques en élaborant une analyse de risque basée sur les acteurs.*
2. *Calculer la probabilité d'occurrence des menaces (acteur, scénario) en réalisant une analyse de risque basée sur les scénarios d'attaque.*
3. *Caractériser le risque encouru par les systèmes en étude en accomplissant une analyse du risque combinée.*

Par le moyen de ce travail de recherche, nous prétendons fournir des orientations au parties concernées sur les vecteurs d'attaque (vulnérabilités) qui doivent être adressées en priorité.

1.5 Plan du mémoire

Dans le chapitre 2 nous effectuons une revue de la littérature des vulnérabilités dont font l'objet certains Dispositifs Médicaux Implantables (DMI) et, des analyses du risque en matière de cybersécurité des DMI. Par la suite, nous expliquons notre méthodologie d'analyse du risque dans le chapitre 3. Les trois étapes dont se compose notre étude y sont décrites en détail à savoir : étape 1) une analyse de risque basée sur l'acteur, étape 2) une analyse de risque basée sur le scénario d'attaque, étape 3) une évaluation du risque combinée. Dans le chapitre 4 nous présentons l'article scientifique *Risk Assessment of Cyber Attacks on Telemetry Enabled Cardiac Implantable Electronic Devices (CIED)* qui a été soumis à un journal. Cet article contient les sorties des étapes ci-avant mentionnées et par conséquent les résultats de notre analyse du risque. Finalement, nous effectuons une brève conclusion dans le chapitre 6 .

CHAPITRE 2 TRAVAUX ANTÉRIEURS

2.1 Menaces affectant les Dispositifs Medicaux Implantables (DMI)

Au cours des dernières années, plusieurs groupes de recherche ont découvert des vulnérabilités au sein de divers types de Dispositifs Médicaux Implantables (DMI). Nous les énumérons chronologiquement dans les paragraphes ci-dessous.

En 2008, Halperin *et al.* [9] ont démontré que les DECI étaient vulnérables aux attaques par radio-fréquence. Les chercheurs ont réussi à inverser le protocole de communication de l'appareil en employant une Radio définie par software (RDS). Ainsi, ils ont été en mesure d'intercepter les données transmissent par un DECI et d'émettre des commandes dangereuses au dispositif.

En 2011, Hei *et al.* [53] ont révélé que les pompes à insuline et les CIED étaient vulnérables aux attaques par épuisement de la batterie. Une fois implantés dans le corps du patient, ces dispositifs communiquent via des ondes RF avec un appareil extra-corporel pour assurer le suivie et le réglage de la thérapie du patient. Ainsi, les chercheurs de cette étude ont démontré qu'en envoyant périodiquement des commandes RF spécifiques à ces DMI, il était possible de maintenir une session de communication ouverte en permanence et par conséquent, de réduire considérablement le temps de service de ces appareils. La même année, Li *et al.* [54] ont démontré qu'une personne non autorisée était en mesure d'interagir avec les pompes à insulines. En effet, leurs travaux ont mis en évidence que certains modèles de pompes à insuline présentent une classe de vulnérabilité qui permettrait à une personne non autorisée d'*émuler toutes les fonctions d'une télécommande : réveiller la pompe à insuline, arrêter/reprendre l'injection d'insuline ou injecter immédiatement un bolus d'insuline dans le corps humain* [14]. La même année, Jérôme Radcliffe, un patient diabétique, a partiellement modifié les protocoles de communication de sa pompe à insuline. Il a annoncé ses conclusions lors de la conférence de cybersécurité Black Hat [13] .

En 2012, le "hacker" Barnaby Jack a dévoilé que certains modèles de DECI peuvent dévoiler leurs données d'authentification suite à la réception d'une commande RF spécifique [55]. Il a également pu vérifier que les données d'authentification de certains DECI sont leurs numéros de série ou de modèle [10, 14]. Cette découverte a mis en évidence qu'une partie non autorisée pouvait prendre le contrôle de certains CIED [10, 14].

En 2016, Marin *et al.* [7] ont analysé les protocoles de communication propriétaires employés par les DECI pour communiquer avec les programmeurs externes. Leurs travaux ont démontré qu'il était possible de maîtriser le fonctionnement des-dits protocoles par le moyen de la rétro-ingénierie. Ce fait met ainsi en évidence l'inefficacité de "la sécurité par obscurité" comme moyen de prévention contre les attaques informatiques. En effet, les chercheurs ont pu réaliser plusieurs attaques informatiques à savoir, le déni de service (DoS), l'usurpation d'identité et les attaques par re-jeu. Les résultats de cette recherche ont été reproduits sur au moins 10 modèles différents de DECI.

2.2 Évaluations du risque en matière de cybersécurité des DMI

2.2.1 Évaluations du risque antérieures

En 2015, Jagannathan et Sorini ont réalisé une évaluation du risque en matière de cybersécurité des dispositifs médicaux implantables (DMI) [56]. Cette étude propose une méthodologie pour évaluer l'exposition des dispositifs médicaux aux risques d'attaques informatiques. La méthode présentée est une étude d'analyse préliminaire des risques (APR) traditionnelle qui a été adaptée afin d'évaluer les propriétés de cybersécurité des équipements médicaux. La méthodologie proposée se compose des trois étapes de base d'une APR, à savoir : 1) l'identification des menaces, 2) la détermination des risques associés à ces menaces, et 3) le classement des risques accompagné des mesures de suivi. Pendant la phase d'identification des menaces, les chercheurs proposent que les composants matériels et logiciels des dispositifs ainsi que les protocoles de communications qu'ils emploient soient rigoureusement analysés. Par la suite, ils recommandent d'élaborer une liste des vulnérabilités trouvées. Lors de la phase de détermination des risques associés aux menaces, le risque est calculé en fonction de l'impact que les menaces ont sur les victimes, et de la probabilité ces menaces puissent se matérialiser. Finalement, dans la phase du classement des risques, les menaces sont classées selon la gravité du risque qu'elles comportent.

En avril 2017, Stine *et al.* [57] ont présenté une méthode d'évaluation du risque de cybersécurité des dispositifs médicaux connectés au réseau. Cette méthode vise à aider les établissements de santé à identifier les dispositifs susceptibles de mettre en danger la santé des patients ou de perturber la qualité de leur suivi. Dans cette étude, les menaces sont classées selon un système de notation et le processus d'évaluation du risque se divise en deux étapes. Dans la première, les dispositifs médicaux sont évalués en considérant qu'ils sont compromis c'est-à-dire qu'ils ont été la cible d'une attaque informatique. Sept types d'attaques informatique ont été considérés : le vol d'identité, la falsification des données, la

répudiation de l'information transmise, la divulgation de données confidentielles, le déni de services, et l'élévation de privilèges. Cette façon de procéder permet de mesurer l'impact que ces attaques auraient sur la santé du patient. Ainsi, compte tenu de la gravité de cet impact, un score initial est attribué au dispositifs évalués. La deuxième étape du processus consiste à distribuer un questionnaire de cybersécurité au personnel médical afin qu'ils évaluent la robustesse des mesures de sécurité qui sont implémentées dans les dispositifs évalués. Ainsi, le score attribué dans la première étape sera ajusté en fonction des réponses au questionnaire. Le questionnaire ci-avant mentionné se base sur le modèle STRIDE développé par Microsoft [58], une mnémotechnique pour aider les développeurs à trouver les menaces qui affectent leurs produits [59].

En mai 2017, Rios et Butts [8] ont analysé l'écosystème des DECI d'une façon exhaustive. Lors de cette analyse ils ont examiné les composants matériels et logiciels de différents modèles de DECI, programmeurs externes et moniteurs appartenant à des fabricants différents. Comme résultat, plus de 800 000 vulnérabilités ont été découvertes. D'après les chercheurs, cela est dû à l'emploi de bibliothèques de tierces parties pour le développement logiciel des produits testés. En effet, bien que l'utilisation de ces bibliothèques accélère considérablement le processus de développement des dispositifs, elle s'avère aussi un risque du fait que dans beaucoup de cas, ces bibliothèques possèdent des failles de sécurité qui n'ont pas été corrigées après la fabrication du DECI. Ainsi, une personne malveillante pourrait exploiter lesdites failles.

En 2018, Abrar *et al.* [60] ont réalisé une analyse pour déterminer si le déploiement des infrastructures des systèmes de santé (ISS) dans le *cloud computing* serait viable sur le plan de la sécurité informatique. Pour ce faire, l'équipe de recherche a premièrement identifié les éléments (systèmes) vulnérables du ISS. Ensuite, ils ont employé la méthode d'analyse du risque OCTAVE [61] pour évaluer l'effet qu'une attaque informatique aurait sur l'intégrité des ISS si leurs éléments vulnérables étaient déployés dans un environnement de *cloud computing*. OCTAVE est une méthode d'évaluation du risque axée sur les processus, elle se compose de trois phases : 1) la vision organisationnelle, 2) la vision technologique, et 3) la planification des mesures et réduction des risques. La vision organisationnelle permet d'identifier les actifs d'une organisation, ses menaces et vulnérabilités, ses exigences de sécurité et, les mesures de sécurité implémentées. La vision technologique quant à elle permet de repérer les composantes clefs de chaque actif afin d'identifier quelles sont les vulnérabilités techniques de ces actifs. Finalement, la planification des mesures et la réduction des risques permettent d'évaluer et caractériser les risques, puis d'élaborer des stratégies de protection.

2.2.2 Évaluation du risque présente vs. évaluations du risque antérieures

Bien que Rios et Butts [8] aient mis le doigt sur les menaces et leur nature, l'ampleur réelle du risque qu'elles comportent n'est pas décrite. Même s'il y a des vulnérabilités dans un système, nous considérons que c'est leur probabilité d'exploitation et l'impact que cette exploitation a sur les individus qui déterminent si la vulnérabilité représente un risque important ou non. Dans cette ligne de pensée, nous avons réalisé une analyse de risque qui, comme les travaux de Jagannathan et Sorini [56], se compose de trois étapes principales, à savoir : 1) une analyse de risques basée sur l'acteur pour identifier les menaces, 2) une analyse de risque basée sur le scénario d'attaque pour déterminer la probabilité d'occurrence des menaces, et 3) une analyse du risque combinée pour caractériser le risque associé aux menaces. Les différences entre leur travail et le nôtre sont que d'une part, nous analysons des dispositifs réels (DECI) et non des dispositifs fictifs comme ils l'ont fait, et que d'autre part, nous estimons le risque d'une vulnérabilité en fonction de la probabilité qu'elle soit exploitée avec succès et de son impact sur les victimes.

Dans le travail de Stine *et al* [57] la probabilité d'exploitation dépend des caractéristiques (mesures) de sécurité mises en place dans les DECI. Dans notre cas, la probabilité d'exploitation sera déterminée non seulement par ces caractéristiques, mais aussi par les ressources externes dont dispose l'adversaire pour réaliser son attaque. Cette procédure nous permet d'inclure des facteurs de risques environnementaux qu'ils n'ont pas pris en compte. De cette façon, nous pouvons estimer le risque que les applications médicales basées sur le nuage peuvent avoir sur la sécurité et la sûreté du patient, de la même manière que le travail d'Abrar *et al.* [60]. Contrairement à toutes les évaluations de risque précédentes, nous mesurons l'impact des attaques à plusieurs niveaux : santé, économie, qualité de vie et vie privée des victimes. De cette manière, notre travail s'adresse à toutes les parties prenantes, i.e. les patients, le personnel de la santé, les fabricants des dispositifs en études et les autorités gouvernementales.

La mesure de l'impact sur la santé suit l'approche de la classification d'Hayes [62]. Cette classification distingue les sources d'interférence électromagnétique susceptibles d'interférer avec les stimulateurs cardiaques en fonction de l'effet clinique que ces interférences peuvent avoir sur l'état de santé des patients. Dans cette étude, 980 porteurs de stimulateurs cardiaques furent exposé aux ondes électromagnétiques émanant de 5 modèles de téléphones cellulaires différents. Tout au long de l'exposition, les patients étaient surveillés par électrocardiographie de façon à ce que, les chercheurs fussent en mesure d'évaluer l'effet que ces interférences provoquaient sur leur état de santé. Par conséquent, les sources d'interférence électromagnétique furent distingués selon trois classes, compte tenu des symptômes

observés chez les patients. La *classe I* regroupe les sources d'interférence électromagnétique provoquant une réponse clinique significative par exemple, celles qui pourraient induire une syncope (perte de connaissance) aux patients. La *classe II* rassemble les sources d'interférence électromagnétique provoquant une réponse clinique probablement significative par exemple, celles qui pourraient provoquer des palpitations au patient. Finalement, dans la *classe III* se trouvent les sources d'interférence électromagnétique provoquant une réponse clinique qui n'est probablement pas significative.

Les impacts économiques, la qualité de vie et la vie privée des victimes ont été mesurés en employant le FIPPS 199 (*Fair Information Practice Principles*) du NIST (*National Institute of Standards and Technology*), un standard pour l'évaluation de sécurité des systèmes de l'information. Ce standard définit les trois objectifs de sécurité que doit garantir toute TIC à savoir : l'intégrité, la disponibilité et la confidentialité de la TIC elle-même et de l'information qu'elle renferme. De plus, le FIPPS 199 définit les trois niveaux d'impact qu'une faille de sécurité pourrait causer chez la victime. Ainsi, l'exploitation malveillante d'une faille de sécurité a un impact bas lorsque la perte de l'intégrité, la disponibilité ou la confidentialité quelle entraîne produit un effet adverse limité chez la victime. L'impact est dit modéré lorsque l'effet adverse est significatif et finalement, l'impact est élevé lorsque cet effet est sérieux.

CHAPITRE 3 MÉTHODOLOGIE

3.1 Méthode d'évaluation du risque

Notre travail se compose de trois étapes : une analyse de risque basée sur l'acteur (Étape 1), une analyse de risque basée sur le scénario d'attaque (Étape 2) et une évaluation du risque combinée (Étape 3) dont les entrées sont les résultats issus des étapes précédentes.

Dans l'analyse de risque basée sur l'acteur (Étape 1), nous déterminons l'impact qui résulte des attaques informatiques contre l'écosystème des DECI. Pour ce faire, nous identifions les potentiels attaquants, i.e. les groupes de cybercriminels qui s'intéresseraient à l'écosystème en étude. Ensuite, nous déterminons les objectifs d'attaque desdits cybercriminels. Cela fait, nous nous servons de la table 4.1 pour déterminer l'impact associé à chaque objectif d'attaque.

Dans l'analyse de risque basée sur le scénario (Étape 2), nous estimons la probabilité d'occurrence des menaces (scénario, acteur). Ainsi, nous commençons par identifier les vecteurs d'attaques, i.e les vulnérabilités exploitables. Ensuite, nous décrivons les scénarios d'attaques menant à l'accomplissement des objectifs d'attaques déterminés à l'Étape 1. Cela fait, nous calculons la probabilité d'occurrence des menaces suivant la formule 3.1.

$$P = c + o + m \tag{3.1}$$

c : Capacité d'attaque de l'attaquant
o : Opportunité pour l'attaquant d'attaquer
m : Motivation de l'attaquant à attaquer

La capacité représente la complexité technique de l'attaque et les ressources techniques et matérielles dont disposent les acteurs pour réaliser la menace. L'opportunité représente les chances de ce dernier d'avoir accès physique à la cible et d'être là au bon moment. La motivation, quant à elle, reflète le degré d'intérêt des acteurs pour accomplir la menace.

$$R = I * P_{MAX} \tag{3.2}$$

I : Impact de l'objectif d'attaque
P_{MAX} : Probabilité maximale par scénario

Finalement, lors de l'évaluation du risque combinée (Étape 3) nous calculons le risque associé à chaque scénario d'attaque, et ceci, compte tenu de l'acteur le plus probable 3,2. Pour ce faire, nous avons employé les résultats d'impact de l'Étape 1, puis les résultats de probabilité maximale par scénario d'attaque de l'Étape 2.

3.2 Expérimentations au laboratoire

Pendant l'analyse de risque basée sur les scénarios d'attaques nous avons réalisé des attaques radio contre un seul modèle de DECI et de programmeur. Par le moyen de ces expérimentations nous voulions déterminer la difficulté technique et la faisabilité de ce type d'attaque dans un environnement réel. Ainsi, ces expérimentations nous ont guidé dans l'estimation de la probabilité d'occurrence des attaques par radiofréquence contre les DECIS ou les programmeurs.

Notre bac expérimental se composait d'outils de différentes natures. Notamment, un programmeur et un DECI tous deux de la marque Biotronik. Le modèle de DECI employé a été un Epyra 8 DR-T, celui du programmeur un Biotronik B.O. Nous avons utilisé une URSP B200, une RDS fabriquée par Ettus Research. Ce modèle est capable de transmettre et de recevoir des signaux dans la plage de fréquences allant de 70 Mhz à 6 Ghz. Étant donné que les RDS nécessitent d'une antenne pour transmettre et/ou recevoir, nous avons employé une SRH-779. Ces antennes sont capables de transmettre et de recevoir des signaux dans des fréquences allant jusqu'à 435 Mhz. Pour le traitement et l'enregistrement des signaux radio, nous avons fait usage des logiciels Gnu-radio [63] et URH (Universal Radio Hacker) [64].

Lors des expérimentations, nous connections l'antenne (SRH-779) a la RDS (URSP B200). Celle-ci était à son tour connectée par câble USB à notre ordinateur. Ce dernier contenant les logiciels de traitement de signaux radio (Gnu-radio et URH). Tout dépendamment de l'attaque que nous voulions réaliser, la RDS était configurée en mode réception (RX) ou transmission (TX). Nous avons réalisé des attaques simples. À savoir, l'interception des communications entre le DECI et le programmeur (Figures 3.1 et 3.2) et des attaques de déni de service (DoS) en émettant du bruit dans les fréquences de travail des dispositifs.

Les résultats de ces expérimentations révèlent que les attaques par radiofréquence ne sont pas techniquement difficiles à réaliser. Nous avons constaté que les logiciels pour traiter les signaux radios sont de plus en plus sophistiqués (plus de fonctionnalités) mais restent faciles à utiliser même pour une personne avec peu de compétences techniques. Cependant, le succès de ces attaques n'est pas évident dans la pratique.

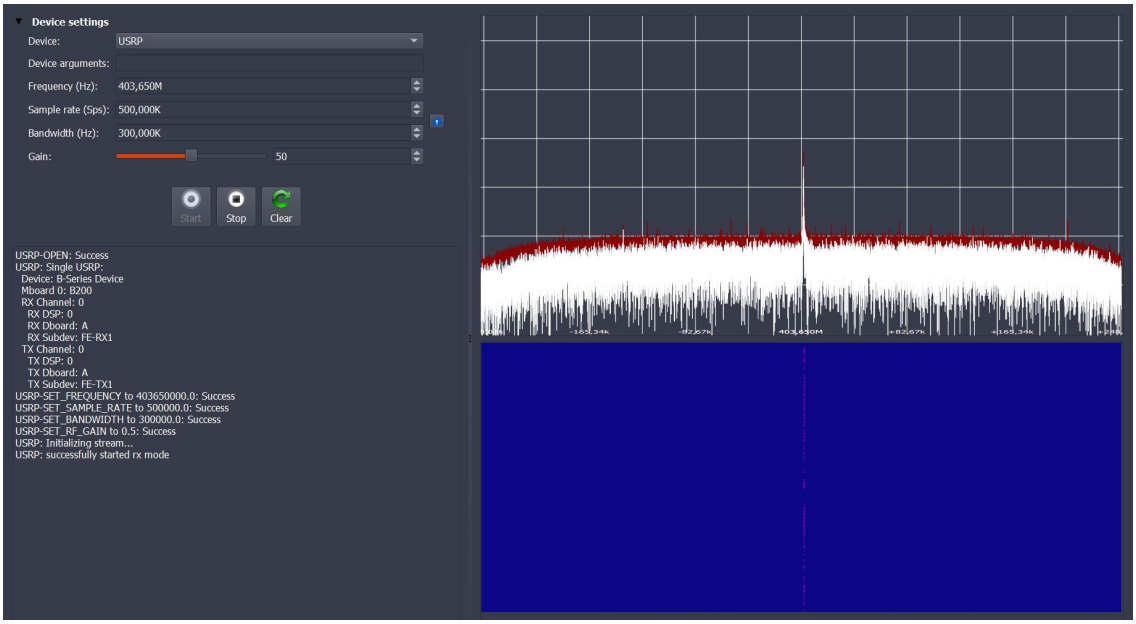

Figure 3.1 Interception des signaux émis par le DECI avec URH

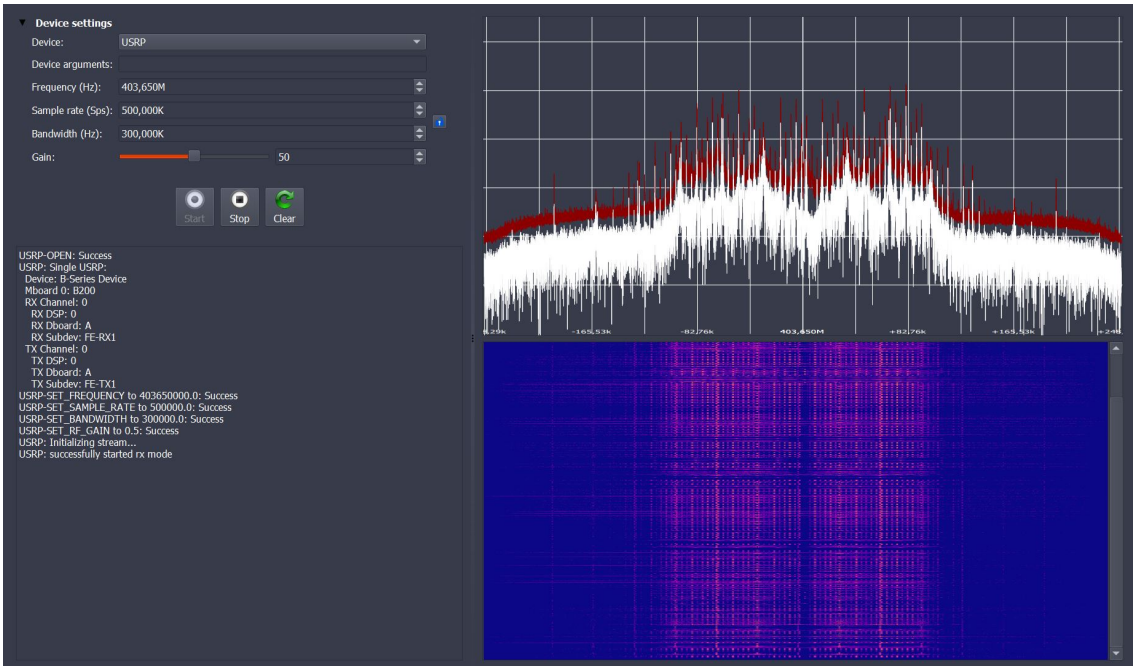

Figure 3.2 Interception des signaux émis par le programmeur avec URH

En effet, lors de nos expérimentations, nous avons remarqué que l'exploitation de l'interface de communication RF (des DECI) via une RDS exige que plusieurs conditions soient simultanément satisfaites. En premier lieu, il faut que l'adversaire soit à proximité de la cible au moment de l'attaque. Comme illustré dans les figures 3.3 et 3.4, la distance entre l'antenne

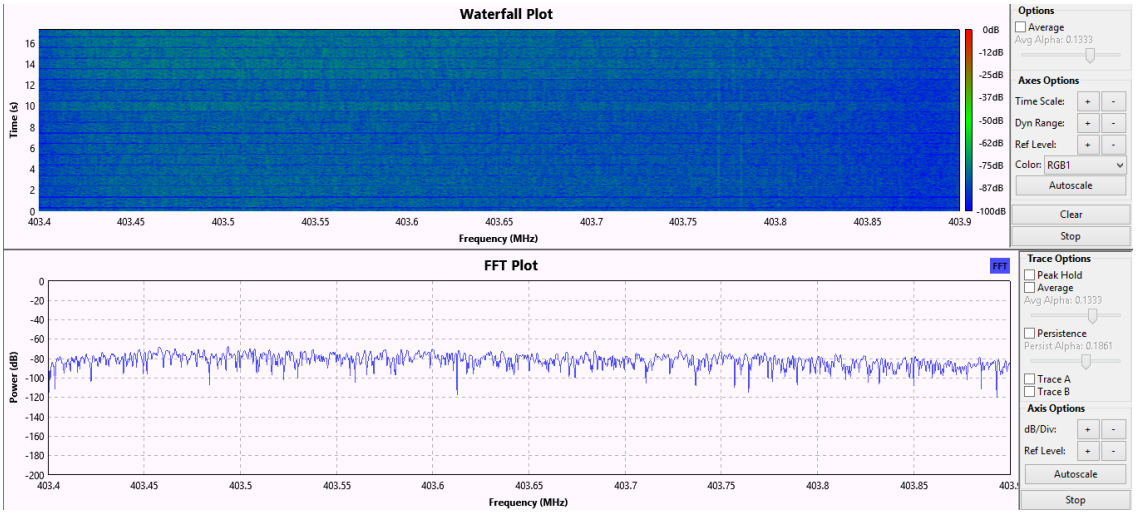

Figure 3.3 Signal du DECI intercepté avec Gnu-radio lorsque DECI et antenne sont à une distance d=0,5 m

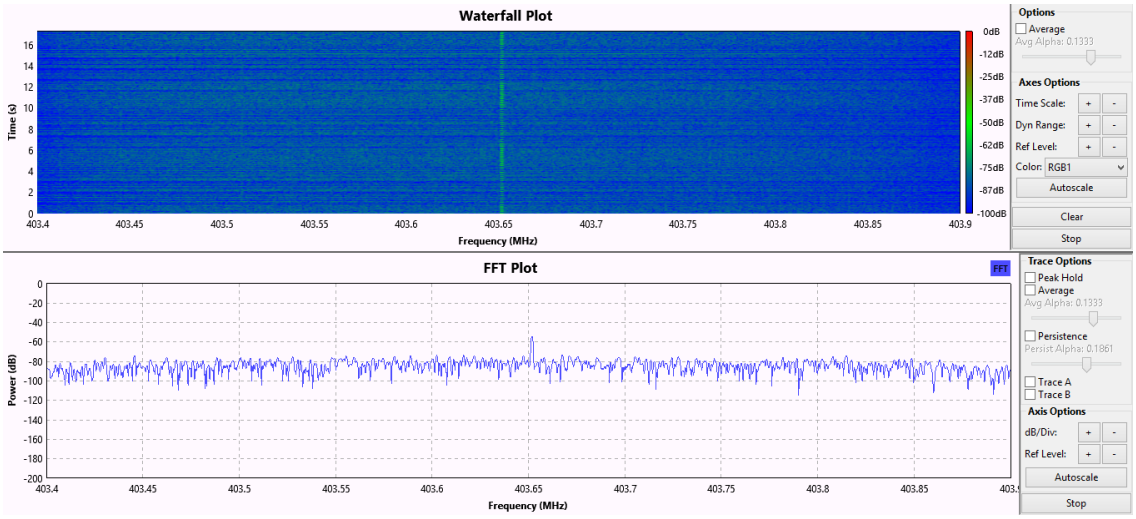

Figure 3.4 Signal du DECI intercepté avec Gnu-radio lorsque DECI et antenne sont à une distance d=0,3 m

et le DECI devait être strictement inférieur au demi-mètre. Contrairement, nous n'étions pas capables d'apercevoir les signaux transmis par le DECI. En deuxième lieu, il faut que l'antenne (émettrice ou réceptrice) soit exactement réglée à la fréquence d'émission du programmeur ou du DECI. Cette prémisse est problématique dans la mesure ou le programmeur et le DECI changent aléatoirement de fréquence de travail d'une session à l'autre. Lors de nos expériences, nous devions faire un balayage de fréquences avec un analyseur de spectre avant de trouver les signaux correspondant aux dispositifs (DECI et programmeur). Cette

opération pouvait prendre quelques minutes si l'un des appareils transmettait à une fréquence située à la fin du canal MICS. Par conséquent, pour qu'une attaque réussisse au premier essai, l'adversaire doit avoir 10 RDS, chacune réglée a l'une des fréquences porteuses du canal MICS. En troisième lieu, la dernière condition concerne le bruit ambiant. Certes, il faut que le bruit ambiant ne soit bas sinon les signaux émis par le DECI ne sont pas apercevables car ce sont des signaux à basse puissance.

Ces conditions réduisent l'opportunité d'attaque des acteurs du fait qu'ils s'exposent à se faire remarquer. Ainsi, comme nous les verrons plus tard, la probabilité d'occurrence des attaques par radio-fréquence n'est pas élevée.

CHAPITRE 4 ARTICLE 1: RISK ASSESSMENT OF CYBER ATTACKS ON TELEMETRY ENABLED CARDIAC IMPLANTABLE ELECTRONIC DEVICES (CIED)

Mikaela Ngamboé[1], Paul Berthier M.SC.A[1], Nader Ammari M.SC.A[1]
Katia Dyrda MD[2], José M. Fernandez PhD[1]

[1]École Polytechnique de Montréal
[2] Montréal Heart Institute, Université de Montréal

Abstract Cardiac Implantable Electronic Devices (CIED) are fast becoming a fundamental tool of advanced medical technology and a key instrument in saving lives. Despite their importance, previous studies have shown that CIED are not completely secure against cyber attacks and especially those who are exploiting their Radio Frequency (RF) communication interfaces. Furthermore, the telemetry capabilities and IP connectivity of the external devices interacting with the CIED are creating other entry points that may be used by attackers. Although the majority of these vulnerabilities are more like proof of concepts or in-the-lab experiments and that there are no indicators of active exploitation or in the wild abuse, it remains crucial to perform a risk analysis to measure how viable these attacks are, their impact and consequently the risk exposure. In this paper, we carry out a realistic risk analysis of such attacks. This analysis is composed of three parts. First, an actor-based analysis to determine the impact of the attacks. Second, a scenario-based analysis to determine the probability of occurrence of each threat. Finally, a combined analysis to determine which attack outcomes (i.e. attack goals) are riskiest and to identify the vulnerabilities that constitute the highest overall risk exposure. The conducted study showed that the vulnerabilities associated with the RF interface of CIED represent an acceptable risk. In contrast, the network and internet connectivity of external devices represent an important potential risk. The previously described findings suggest that the highest risk is associated with external systems and not the CIED itself. A noteworthy observation that emerged from the risk analysis is the fact that the damages of these cyber attacks could spread further to affect parties other than patients such as device manufacturers through intellectual property theft or medical practitioners through affecting their reputation.

Preprint submitted to Computers & Security

This research work has contributed to extend the knowledge in terms of quantifying the risk associated not only to CIED devices but also to their ecosystem. The results of this study could be considered as a base for CIED risk management procedures as they help to measure the impact of different attacks while taking into consideration the attackers goals, identifying attack scenarios as well as their likelihood of occurrence and determining which threat has to be addressed in priority.

Keywords Cardiac Implantable Electronic Device, CIED, cyber security, cyber attack, vulnerabilities, attack vectors, attack scenarios, actor-based risk analysis, scenario-based risk analysis.

4.1 Introduction

Cardiac implantable electronic devices (CIED) have evolved from single-chamber pacing devices to resynchronization and defibrillation within the same device [4]. Modern CIED now include numerous functionalities being integrated into a single device, which has contributed to an increase in the number of implanted devices [5,6]. Besides, the use of telemetry-enabled CIED is increasing at the detriment of older models with no wireless-communication capabilities [24, 25], due to the significant advantages it brings to patient care [27, 28]. For the remainder of this article, the acronym CIED will refer only to telemetry-enabled CIED.

CIED interact with external systems located in the hospital (the *external programmer*), the patient's home (the *home monitor*) and in the cloud [8, 24, 26]. They communicate with the external programmer and the home-monitoring device via Radio Frequency (RF) signals transmitted in the Medical Implants Communication Services band (MICS 402-405 Mhz) [5, 65–68], whereas they interact with cloud-based systems by means of the home-monitoring device and Internet Protocol (IP) connectivity [26–28].

External programmers are used by the physicians *ab initio* when configuring the devices prior to implantation and during patient follow-up sessions to retrieve data and for reconfiguration. They have three modes of operation: 1) the *interrogation mode* to check a patient's cardiac programmed parameters and stored data, 2) the *test mode* to test that the implant is operating properly, and 3) the *programming mode* which allows the physician to adjust the patient's therapy by reconfiguring the functionality of the CIED [24,25]. Reconfiguration after manufacturing is feasible since current CIED circuitry is microprocessor-controlled and its software can be updated [6, 18–23, 34].

Home monitoring devices are intended to supervise the patient's cardiac status. They period-

ically collect activity data from the CIED and send it to a cloud-based database. The latter may be operated by either the CIED manufacturing company or a web services provider used by the physician to access the patient's data [26–28].

As evidenced by previous work, CIED are vulnerable to cyber attacks that use their RF interfaces to communicate with the devices [7, 9]. This is also true for non-telemetry enabled CIED, but telemetry introduces additional vectors of cyber attacks that can include manipulation of the home monitor, interception of transmissions from the home monitor to the cloud and the physician's station, and manipulation of the cloud-based database itself [8, 14]. Proof of the increased concern of cyber attacks on CIED was given by the recall of almost half a million CIED by the Food and Drug Administration (FDA) in August 2017. According to the FDA, the aforementioned devices were vulnerable to unauthorized access, allowing a malicious person to reprogram them using commercially available equipment [11]. However, no such attacks have been reported. While we know it would be technically possible to conduct such an attack in the controlled environment of a research laboratory [7–9], it remains to be determined how viable such an attack would be on an actual target in the real world. This is precisely our research question: What are the real-life risks of cyber attack onto telemetry-enabled CIED and the systems they depend on?

In this work, we carry out a realistic risk analysis of such attacks, with regards to actual impact these problems pose in terms of: health, economy, quality of life and privacy of the affected parties. In order to carry this risk analysis, we inventory the vulnerabilities that have been made public up to now, we define attack scenarios based on them, describe and evaluate the impact of the various attack goals that various actors would want to achieve through such attack scenarios, and finally estimate the likelihood of occurrence of each of these attacks to determine overall risk.

Our motivation to conduct this research is based on the need to understand the real scope of the problem. After the FDA statement was released, patients began to massively call their cardiologists to get an explanation about these potential failures and to what extent they were in danger. It is at times difficult for physicians to answer them, since cybersecurity is not their field of expertise and because there is little information about the clinical impact of exploitation of the vulnerabilities found. This is why we believe that such a "reality check" is necessary, as the real scope of the problem it is not clear at all. By determining the scope of the problem we contribute to 1) extend the knowledge of the threats affecting CIED, 2) provide guidance on which threats should be addressed in priority and consequently 3) provide to the organizations potentially interested in this kind of risk assessment a basis from where to start, e.g. health regulation agencies, device manufacturer, health practitioners, etc.

4.2 Background on CIED

4.2.1 CIED computer-based architecture

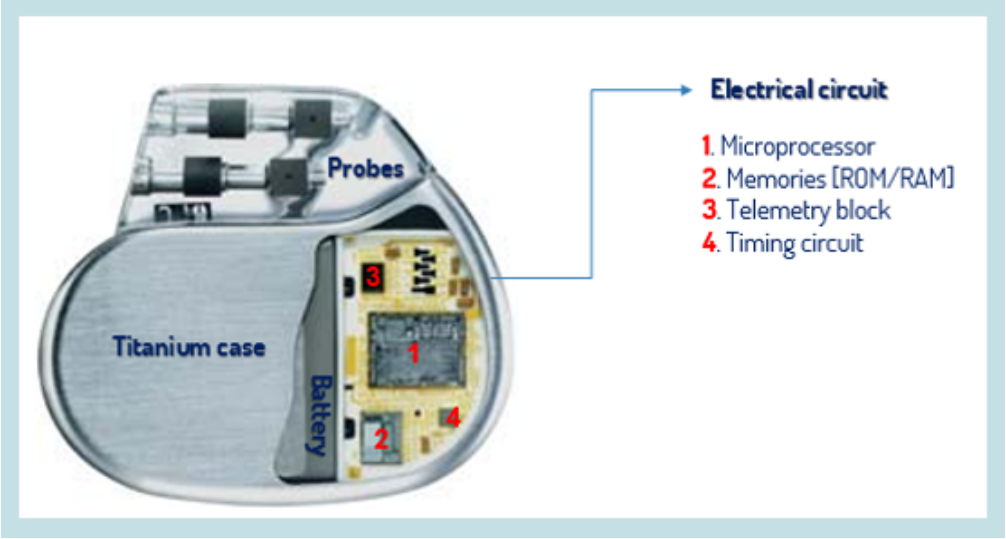

Figure 4.1 CIED circuitry

Few documentary sources on CIED architecture and design are available, due to the proprietary nature of that information. Nonetheless, common principles and some technical details are generally documented in some of the corresponding patents [6, 18–22]. As depicted in Figure 4.1, today's software-based CIED circuitry is mainly composed of four electronic components with the first one being the *microprocessor* which is the "brain" of the CIED. It coordinates, controls and directs the interactions between the elements of the circuit. It also interprets and executes the algorithms programmed in memory. The second component is the *memory*, CIED holds two kinds of memories: Read-Only Memory (ROM) and Random-Access Memory (RAM). The ROM contains the embedded software (also known as *firmware*) providing low-level control of the device's hardware, as well as the code implementing the various functionalities of the device. While the RAM is taking care of storing a variety of parameters, such as device serial number, patient ID, clinical information, patient's cardiac activity (arrhythmia logs, frequency histograms) and certain programs implementing particular therapies. The third component dubbed the *telemetry circuitry* is used to establish a communication link between the CIEDand external devices, such as the external programmer or a home monitor. More specifically, the telemetry circuitry allows performing remote monitoring, therapy adjustment and reprogramming the CIED prior to implantation or during patient follow-up sessions. The fourth electrical component is the *timing circuit* which is a

key element on the CIED circuitry as it takes care of synchronizing the stimulation pulses to the cardiac chambers as well as the memory access.

The previously described components are interacting together to maintain the CIED functionalities, each one of them has a specific task that has to be executed in a coordinated way. A good example of these multi-component interactions would be the automatic therapy selection loop (Figure 4.2). This process is performed at the microprocessor level using signals coming from the detection probes that are continuously monitoring and re-transmitting the cardiac activity to the microprocessor. The re-transmitted signals are then interpreted in order to select the adequate therapy code from the RAM. Finally, the selected code is translated to a low-level instruction set (located in the ROM) before being executed by the microprocessor. It is also important to mention that the treating physician is responsible of determining which therapies can be applied under what conditions.

The clinician uses the programmer's user interface to program or adjust the parameters of the patient therapy (i.e., number of beats per second). When fixing a therapy parameter on the programmer user interface, the external device subsequently sends to the CIED an instruction containing the change to perform on the therapy. The telemetry circuitry receives this instruction and then sent it to the microprocessor. Following the interpretation of the instruction, the microprocessor will access the RAM to perform the required change. (Figure 4.3).

4.2.2 CIED ecosystem

The CIED ecosystem (Figure 4.4) encompasses the set of devices, cloud-based systems and cloud-based services employed for the diagnosis, the therapy's adjustment and the monitoring of patients with an implanted CIED. Apart from the CIED itself, there are two other medical devices forming part of this ecosystem. These are, the external programmer usually located at the hospital and the monitor located at the patient's home. Health professionals rely on the external programmer to obtain the programmed parameters of the patient, to adjust the desired therapies or to check the correct operation of the CIED [24, 25]. The home monitor is used to periodically collect the data stored in the CIED and send them to a cloud-based database (DB). Thus, medical staff can access a patient's health information through a web-based application, operated either by the CIED manufacturer or a separate cloud service provider [26–28]. It is fair to say that the monitor is a key element of this system of systems as it is through him that some CIED data are available on the cloud-based elements of the ecosystem in study. By cloud-based elements, we refer to the cloud-based database containing the information coming from the monitor, the cloud-based application displaying

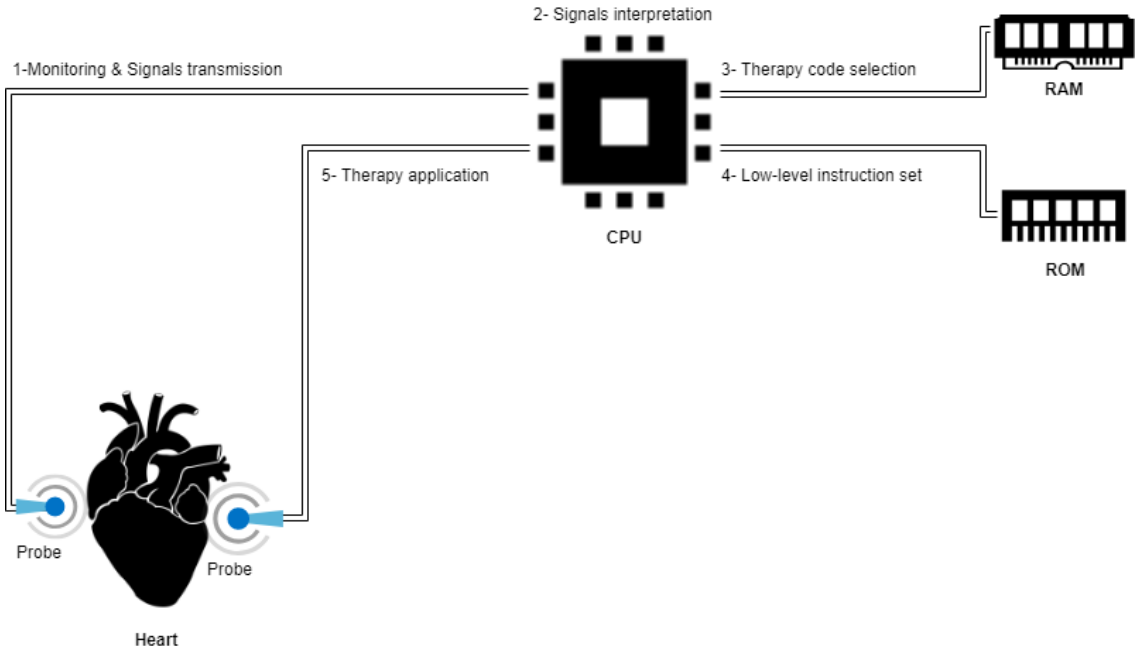

Figure 4.2 Therapy selection loop

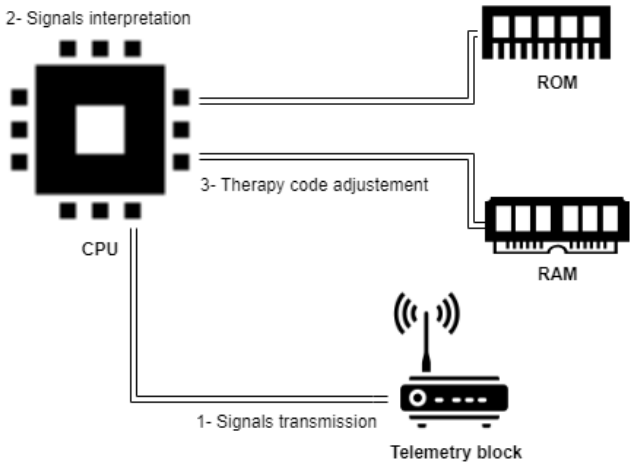

Figure 4.3 Therapy adjustment

this information and, the cloud-based server containing the application. Moreover, the set of devices employed to use the application mentioned above (e.g. smart-phones, tablets, and laptops) form also part of the ecosystem of CIED.

The CIED interact with all the elements of their ecosystem. Depending on the element, the interaction could be either direct or indirect. Direct interaction takes place with both the external programmer at the hospital and the home monitor device, while indirect interaction occurs with the cloud-based systems and services. We distinguish the type of interaction since as we will see later (Section 4.6.2), it determines the kind of attacks that can be carried out.

Direct interaction consists of wireless communication between the CIED and a programmer or a home monitor device. Indeed, current pacing devices include two types of wireless technology. The first, referred to as *Inductive-coil telemetry*, uses an inductive RF field (0-300 kHz) to communicate over short ranges (0-10 cm), requiring proximity between the CIED and the antenna coil of the external programs. The second mode referred to as *RF-link telemetry*, uses a radiating RF field (i.e. traditional RF waves) at a higher frequency (402-405 MHz) to communicate over longer ranges (0-200 m) [69]. Both technologies can be used for interrogation and programming operations during follow-up visits at the hospital. The main difference between them is that with inductive coil telemetry it is necessary to apply a programming head [1] right above the CIED to establish communications, while with RF link this can be achieved without such proximity; it is therefore referred to as “wandless" [24, 25]. Nowadays, the trend is to use RF-link telemetry to the detriment of the inductive-coil telemetry, since it has a better conductivity in the human body, a higher data rate, a greater communication range, and thus constitutes a more adequate option for home monitoring [24,25]. This technology operates on the Medical Implant Communications Service (MICS) core band (402-405 MHz) initially allocated by the Federal Communication Commission (FCC) in 1999 [67], and that has subsequently been adopted in different regions of the world [5, 65].

The MICS spectrum was established in order to support data transmission between any implanted and external device for diagnostic and therapeutic purposes, not only for CIED [65,68]. However, since this band is shared with communication devices used by meteorological services, its use has been normalized to avoid any interference [5, 66, 67]. These rules of use are based on ITU-R Recommendation [2] SA.1346 [70], whose broad outline is the following:

1. A programming head is an sub-component of the programmer serving as a security switch that can activate or deactivate data transmission to/from the CIED.
2. The ITU-R Recommendations are international technical standards elaborated by the Radiocommunication sector of the International Telecommunication Union.

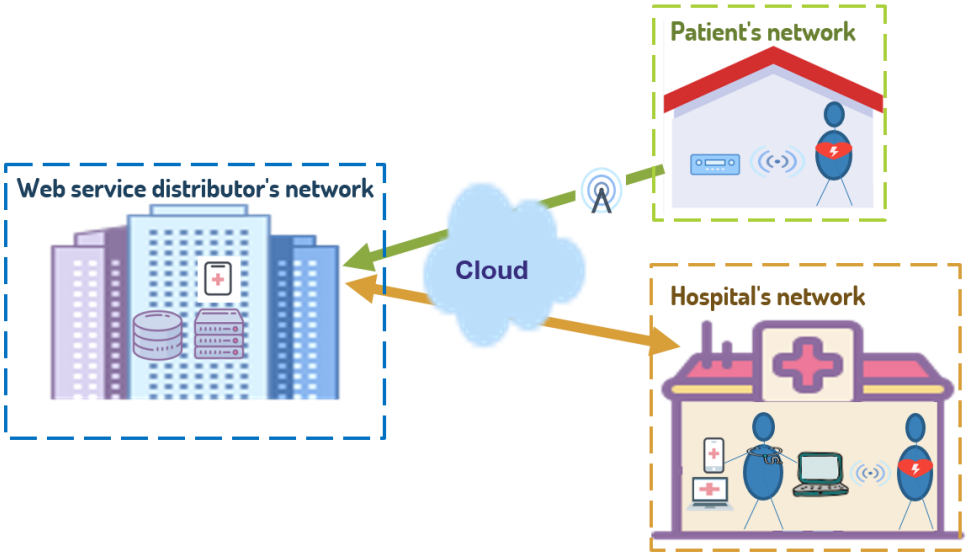

Figure 4.4 CIED's ecosystem.

— The MICS spectrum is divided into 10 transmission channels with a bandwidth of 300 kHz each.
— The implanted devices can only transmit after receiving a command from an external device authorizing them to do so (there are exceptions such as emergencies).
— External devices must integrate interference mitigation techniques, such as Listen Before Talk (LBT) and Adaptive Frequency Agility (AFA) to minimize the effect of ambient noise. External device radio transmitters use LBT to sense their radio environment before starting a transmission, in order to identify a free channel with least interference, i.e. the Least Interference Channel (LIC). Channel verification is done five seconds before initiating a transmission, with each channel being monitored for 10 ms to determine if it is occupied. Then, based on the sensed information the transmitters use the AFA technique to select an operating frequency that is not in use yet [71, 72].

Although the use of the transmission means adheres to an internationally-adopted standard and is carefully regulated, the same cannot be said for signal-conditioning techniques or CIED access control mechanisms. While the Health Insurance Portability and Accountability Act (HIPAA) [3]determines privacy and security rules for the protection of medical data transmit-

3. The HIPAA was created in 1996 to enhance the performance of the U.S healthcare system. The progressive adoption of IT in the health services has led to the inclusion of security and privacy rules on the HIPPA. Those rules protect the sensitive data of the patients that are electronically stored or transmitted .

ted between systems, these remain very general and are more oriented towards traditional Information Technology (IT) systems such as computers and servers. While the FDA has defined good practice guidelines in this area, they do not *establish legally enforceable responsibilities* [73, 74] so their application remains optional. This legislative vacuum results in an overabundance of proprietary communication and authentication protocols, where it is up to each manufacturer to set their own criteria and choose the security methods to apply to their devices.

Indirect interaction occurs between the CIED and the cloud-based systems or services when those are employed to display the information contained in the CIED. Health practitioners have the ability to access the collected data using their own portable devices via connection to the cloud-based web application through a regular Internet connection. This approach aims to improve the quality of patient care and the working conditions of medical staff while reducing health costs. Thus, even if strictly speaking there is no direct communication between the CIED and these systems, there is still a data link between them. Nonetheless, current CIED features do not include the capability to download information from the DB server, and in principle cannot be remotely reconfigured by the health practitioners from the monitors.

In summary, CIED operate in a complex and heterogeneous ecosystem composed of various devices connected to different networks and using multiple communication protocols to interact with each other. The necessity to reduce health costs is propelling a worldwide transformation of health service management that relies precisely on the interaction between medical devices and health practitioners. Nevertheless, this interaction, which is undoubtedly beneficial for all stakeholders, may have turned into a significant attack surface for cyber attacks against the CIED ecosystem [75].

4.3 Background on Implantable Medical Devices (IMD)cybersecurity

The security threats that affect CIED apply to all IMD. The latter are vulnerable to malicious exploitation of (i) their RF communication interfaces, and (ii) the telemetry functionalities and IP connectivity of the extracorporeal equipment on which they depend. In this section, we develop a critical review of the literature on cyber threats affecting IMD and risk assessments regarding IMD risk exposure to cyber attacks. We proceed in this way for two reasons. First, there is no abundant and exclusive literature on the cybersecurity threats of CIED. Second, we claim that the risk assessment methodology proposed here applies to all IMD.

4.3.1 IMD Cyber Threats

In the last decade, several research groups have exposed vulnerabilities in implantable medical devices (IMD), such as insulin pumps and, of course, CIED. Below, we chronologically describe these findings.

In 2008, Halperin *et al.* [9] unveiled CIED vulnerabilities to radio frequency-based attacks. By making use of a software-defined radio (SDR), the researchers succeeded in reverse engineering the device's communication protocol and conducting attacks such as sensitive data interception and dangerous command emission (electric shock dispensation).

In 2011, Hei *et al.* [53] found vulnerabilities that allow resource depletion attacks on insulin pumps. They demonstrated that by sending periodic wireless commands to the IMD, it was possible to keep an active communication session permanently opened, thus significantly reducing the device's service lifetime. During the same year, Li *et al.* [54] disclosed insulin pump vulnerabilities that allow unauthorized parties to communicate with the device. In fact, their work revealed that some insulin pump models possess a class of vulnerability that can allow an unauthorized party to *emulate the full functions of a remote control: wake up the insulin pump, stop/resume the insulin injection, or immediately inject a bolus dose of insulin into the human body* [14]. That same year, Jerome Radcliffe, a patient with diabetes, partially reverse-engineered the communication protocols of his insulin pump. He announced his findings at the Black Hat cybersecurity conference.

In 2012, the hacker Barnaby Jack demonstrated that certain CIED models can disclose their authentication credentials following the reception of a specific command [55]. He was also able to verify that the access codes of some devices are simply their serial and model number. Paradoxically, this information is disclosed by some CIED models when they receive a specific command from an external programmer or a home-monitoring device. This discovery highlighted that an unauthorized party could gain control of certain CIEDs by simply sending a command [10, 14].

In 2016, Marin *et al.* [7] used a black-box reverse-engineering [4] approach to analyze the proprietary communication protocols employed by CIED to communicate with external programmers over a long-range RF channel. Their work evidenced that reverse-engineering CIED proprietary communication protocols is feasible and that they present several implementation weaknesses. As proof of that, they were able to implement a set of exploits like the interception of sensitive information, Denial-of-Service (DoS), spoofing and replay attacks. The findings of this research were reproduced for at least 10 different models of CIED.

4. Method by which an attacker discovers the structure and function of a software by interacting indirectly with it, for example through input and output vectors, libraries or APIs.

4.3.2 IMD cybersecurity risk analysis

Even though the first study evidencing vulnerabilities in CIED was published in 2008 [9], it is only in 2015 i.e seven years later that the first IMD risk assessment study appears in the literature.

In 2015 Jagannathan and Sorini conducted a full IMD-specific cybersecurity risk analysis [56]. This study presents a methodology to evaluate medical devices exposure to cybersecurity risks. The method presented is a traditional Preliminary Hazards Analysis (PHA) study which was tailored to assess the cybersecurity properties of medical equipment. As any PHA study, their methodology consists of three main steps namely: 1) hazard identification, 2) risk determination, and 3) risk ranking and follow-up actions. This work analyses the cybersecurity risk of fictitious medical devices. Thus, its findings do not reflect the actual state of the problem. In our work, we analyze real medical devices that are currently in the market. Therefore, the results herein find not only illustrate the actual scope of the problem but can serve as a basis for the risk management procedures related to the CIED ecosystem.

In April 2017, a study by Stine *et al.* [57] presented a cybersecurity risk assessment method for network-connected medical devices. This study introduced a scoring system relying on a cybersecurity questionnaire based on the STRIDE [5] model developed by Microsoft for classifying threats [58]. The scoring system is intended to help healthcare organizations in identifying those medical devices that have the potential to endanger patient health or disrupt the quality of medical follow-up. This study estimates the probability of occurrence of an attack according to the security features implemented in the target system. Since the estimate of P is only based on the technical difficulty of the attacks, it does not adequately reflect reality. Just because an attack is technically simple to carry out does not mean that an attacker will be interested in achieving it. The chance and willingness to attack are essential factors when it comes to estimating P. Accordingly, in our study, we estimated P in function not only of the characteristics of the target system but also, in function of specific characteristics of the attacker.

In May 2017, Rios and Butts [8] conducted an exhaustive analysis of the CIED ecosystem and the interdependence between its elements. The hardware and software components of different models of CIED, external programmers and home-monitoring devices from different manufacturers were examined. As a result, over 8,000 known vulnerabilities were discovered in third-party libraries of four external programmer models belonging to four different manufacturers. Besides, vulnerabilities were found in all CIED evaluated. The publication of

5. STRIDE is the acronyms of a set of computer attacks namely Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege

this work preceded the massive recall of CIED ordered by the FDA in August 2017, based on the vulnerabilities reported by the Industrial Control Systems Computer Emergency Response Team (ICS-CERT) of the US Department of Homeland Security (DHS). This work identifies the threats and their nature however, the real scope of the risk that those threats entail is not described. We consider that although there are vulnerabilities in a system, it is their probability of exploitation and the impact that this exploitation has on individuals that determines whether the vulnerability represents a significant risk or not. In our study, we estimate the risk of a vulnerability based on the probability that it will be exploited and, the impact that the exploitation will have on victims.

In 2018, Abrar *et al.* [60] conducted a risk analysis on cloud computing within the context of health applications, in order to evaluate their suitability for the Health Infrastructure System (HIS). The research team identified HIS vulnerabilities and then analyzed the impact that a security breach would have on its integrity if the vulnerable elements were deployed in a cloud computing environment. This paper analyzes a mortgage situation, while we analyze a real situation, i.e. the risk that current CIED cloud-based services represent for patient safety.

Our cybersecurity risk assessment is divided into three analysis: 1) actor-based analysis, 2) scenario-based analysis and 3) combined analysis. On the first one, we identify the potential actors and determine the impact of the attacks according to four separate aspects: health (H), monetary (M), privacy (P) and quality of life (QL). Thus, the outcomes of this work may support the objectives of different kind of organizations potentially interested in CIED risk assessment, e.g. health regulation agencies, device manufacturer, health practitioners, etc. On the second analysis, We determine the attack scenarios and then estimate their probability of occurrence according to the actors capacity, opportunity and motivation to achieve the attacks. Finally, in the last analysis, we calculate and characterize the risk associated with each threat (actor, scenario).

4.4 CIED ecosystem's cybersecurity risk assessment methodology

4.4.1 Aim of the risk assessment methodology

The number of IMD that rely on ICT to ensure patients therapy, diagnosis or follow-up is increasing. However, unlike traditional ICT systems (computers, servers, networks...), there is not yet a formal and effective method to assess the cybersecurity risk incurred by IMD. As mentioned in section 4.3, even if the first vulnerabilities were found in 2008, it is only recently in 2015 that the first IMD risk assessment appears in the literature. Therefore, this

area of study is just starting to develop, hence the need for a methodology.

In this work, we propose a method for asses the cybersecurity risk incurred by CIED, a subcategory of IMD. Our method can be used to guide organizations interested in conducting risk assessments of CIEDs and can be extended to other IMD.

4.4.2 Definitions

We define here the cybersecurity and risk assessment terms used in this article.

Actor: A person or organization that violates the integrity, privacy or confidentiality of a computer system‘s data to obtain a benefit.

Impact: Quantification of an attack's effect or consequence on the target or victim.

Victim: A person or organization that is the subject of a computer attack.

Attack goal: Final effect desired by the actor, resulting in a negative impact on the target system or victim.

Scenario: Set of actions carried out by the actor to achieve his attack goal.

Threat: A combination of a person with deliberate intent (actor) comitting acts in particular fashion (scenario), resulting in a negative consequence (impact).

Vulnerability: A design, manufacturing or programming flaw in a system that may offer the opportunity to conduct an attack on it.

Attack vector: Subset of vulnerabilities for which there is a demonstrated attack method by which the vulnerability is employed (exploited) by the actor to reach its final goal or an intermediate goal towards it (e.g. gaining access).

Exploit: Subset of attack vectors related to software vulnerabilities.

Probability: Likelihood that a particular threat (a given actor successfully reaching an attack goal through a given scenario) be materialized during a given period of time.

Risk: Quantification of a threat (Risk = Impact * Probability).

4.4.3 Risk assessment methodology

Our risk assessment methodology is divided into three steps:

Step 1. Actor-based risk analysis In this phase, we aim to determine and quantify the impact of attacks on the CIED ecosystem. To do this, we first identify potential actors that would be interested in attacking the CIED ecosystem. Then, we determine

Table 4.1 Impact levels

Type	Level	Description of the Impact
Health	1	Minor harm to the patient
	2	Significant harm to the patient not involving serious life threatening injuries
	3	Severe harm to the patient that involve serious life threatening injuries
	4	Catastrophic harm to the patient that involve loss of life
Monetary	1	Minor monetary loss
	2	Significant monetary loss
	3	Severe monetary loss
	4	Catastrophic monetary loss
Quality of life	1	Minor impact on the patient's quality of life
	2	Significant impact on the patient's quality of life
	3	Severe impact on the patient's quality of life
	4	Catastrophic impact on the patient's quality of life
Privacy	1	Minor impact on the patient privacy if information is disclosed
	2	Significant privacy impact if information is disclosed
	3	Severe impact on the patient privacy if the information is disclosed
	4	Catastrophic impact on the patient privacy if the information is disclosed

their likely attack goals and from there we quantify the impact on the victim of the successful accomplishment of such attack goals. We do this separately according to four different categories of impact: Health, Monetary, Quality of Life and Privacy. We measure the impact on health by applying the Hayes classification approach [62] that was introduced to classify the impact of different levels of clinically significant electromagnetic interference with pacemakers. The monetary, quality of life and privacy impacts are measured using the Fair Information Practice Principles 199 (FIPPS 199) from the National Institute of Standards and Technology (NIST). The FIPPS 199 is a standard for assessing the security of information systems. The impact is quantified according to a four-level scale described in Table 4.1 and discussed in more detail in Section 4.5.3.

Step 2. Scenario-based risk analysis Here, we estimate the probability of occurrence of various threats. We start by identifying attack vectors, i.e. exploitable vulnerabilities, associated with CIED. We found those attacks vectors on the literature [7–9, 53], the ICS-CERT advisories [12, 35, 39], the National Vulnerability Database (NVD) maintained by the NIST, and the Common Vulnerabilities and Exposure (CVE) database maintained by the Mitre Corporation [36–38,40,50–52,76] . Next, we describe how these attack vectors can be strung together into a series of actions, i.e. attack scenarios, that lead to the achievement of the attack goals (determined in Step 1). Once this is done, we calculate for each threat, i.e. each (actor, scenario) pair, its

probability of occurrence according to the formula

$$P = c + o + m \tag{4.1}$$

where c, o, and m represent, respectively, an assessment of the actor's *capacity*, *opportunity* and *motivation* to conduct the attack scenario described. More precisely, capacity takes into consideration the technical complexity of the attack scenario and the technical and material resources available to the actors to carry it out. The opportunity represents the actor's chances of having physical or network access to the target and being there at the right time to exploit an attack vector and conduct subsequent scenario actions. Finally, motivation captures the inherent likelihood that the actor will put the resources in place and attempt to conduct the attack scenario given what he stands to gain from successful accomplishment of the attack goal.

Step 3. Combined risk assessment In this last step, we calculate the overall risk associated with each attack scenario based on the most likely actor.

$$R = I * P_{\text{MAX}} \tag{4.2}$$

Where I is the impact calculated from Step 1, and P_{MAX} is the maximum actor probability for each attack scenario, as determined in Step 2.

4.5 Actor-based analysis

4.5.1 Potential actors

The ICS-CERT has characterized a *cyber threat source* as "*persons who attempt unauthorized access to a control system device and/or network using a data communications pathway*" [77]. It further classifies these threat source into four groups (A1 through A4):

A1. Cybercriminals groups This includes traditional cybercriminals groups that use compromised computer systems to commit identity theft and online fraud of various kinds, mostly for monetary gain.

A2. Industrial spies Organizations that use computer tools to illegally acquire intellectual property, know-how, trade, and commercial secrets, or other kinds of corporate confidential information. This kind of espionage occurs between competing corporations, for economic reasons.

A3. Foreign Intelligence Agencies Foreign state-based organizations that use computer tools to acquire sensitive information on opposing states, corporations or individuals, or otherwise influence their actions.

A4. Terrorist groups Organizations seeking to create public disorder or sow national terror, by committing destructive violent acts.

While this taxonomy of cyber threat sources was introduced for traditional threats to IT infrastructure, we nonetheless proposed to use them in the context of cyber threats against the CIED ecosystem. To that effect, and considering the likely objectives [75] and motivations [77] of these actors, we maintained the six kinds of attack goals (G1 through G6) described herein.

4.5.2 Attack goals

G1. Access patient sensitive data

CIED ecosystem devices are an attractive target because they constitute a rich source of information. Beyond medical data, they store other types of information such as email addresses, residence addresses, telephone numbers, social security numbers, etc., attractive to many actors. On the one hand, intelligence services (A3) and terrorist groups (A4) would be interested in having this information because it would allow them to attain their ultimate goal (surveillance, assassination, etc.). On the other hand, cybercriminal groups (A1) would be interested to leverage this information to obtain monetary gain since the medical data of individuals is highly valued in the black market [78–81]. Their clients could be for example insurance companies (medical or automotive) that may use this information to assess the cost of insurance premiums or simply refuse coverage.

G2. Gain knowledge of device operation and software

There is significant competition between medical-device manufacturers because of its high-profit margins and high barriers to entry in the market [82,83]. Accordingly, CIED ecosystem devices could be a target for industrial spies (A2) aiming to obtain intellectual property on device design, software and other kinds of engineering details. Subsequently, such information could be sold to competing medical-device manufacturers or possibly to counterfeit medical devices manufacturers in less regulated countries (similarly to the production of counterfeit or generic pharmaceutical products). Furthermore, this information is also valuable for criminal groups (A1), intelligence services (A3) and terrorist groups (A4) because it allows them to undertake attacks by maliciously exploiting the device characteristics or operating mode.

G3. Induce medical staff to make errors

Health is one of the main factors of concern for individuals. Hospitals and their personnel are highly valued in society because individuals trust them [84–87]. Some attackers may be interested in damaging the reputation of health centers or professionals to sow distrust and fear in the society. These could include foreign intelligence services (A3), terrorist groups (A4), or even cybercriminal groups (A1). Apart from sowing fear, said actors could be interested in harming a particular, targeted person. Thus, inducing medical staff to make errors not only would they be achieving their goal, but they would also be evading the responsibilities of their actions by making their interference less detectable.

G4. Disrupt or lower quality of patient follow-up

Cybercriminal groups (A1) could be attracted by those kinds of attacks to realize extortion, industrial or corporate sabotage. The first objective would be to disrupt or even interrupt a healthcare provider's service to demand money to restore it. The second would be to interfere with a targeted CIED manufacturer in order to make believe that their CIED equipment is defective, thus damaging the company's sales revenue and reputation. The third would be to damage the reputation of a targeted health center or professional. For example, disrupting the quality of a target center's patient follow-up could decrease public and government trust in the institution, and lowering its chances of getting adequate revenue and allocation of public resources. Intelligence services (A3) or terrorists (A4) could be motivated to conduct such attacks to harm the population of an opposing country.

G5. Alter device behaviour to endanger patient

This constitutes the most potentially worrisome outcome of the cyber attack against the CIED ecosystem. Indeed, by changing the device settings so that it has an unexpected or dangerous behavior, actors could seriously endanger a patient's life. It is conceivable that foreign intelligence services (A3) and terrorist groups (A4) targeting particular high-value or highly-visible individuals might be motivated to use this kind of attack for assassinations or as a form or extortion or ransom.

G6. Alter device behaviour to decrease quality of life

For the same reasons described above, intelligence services (A3) and terrorist groups (A4) could be motivated to use similar methods to accomplish non-lethal disruptive effects on patients by forcing them to repeatedly visit the clinic due to device malfunction, generate

false alarms, or otherwise tampering with device configuration. Beyond serious harm, such disruptions could be used to mine the confidence of the population on health providers, device manufacturers, or create panic and terror (A3 and A4). The possibility should also be considered that cybercriminals (A1) migrate from traditional forms of IT-based extortion, such as file-encrypting ransomware, to medical device-based extortion, e.g. by locking out access by health practitioners to a patient's CIED and demanding a ransom to restore it.

In summary, the vulnerability of the CIED ecosystem to cyber attacks is a matter of concern not only for patients but also for other groups such as health practitioners, medical device manufacturers and government in general.

4.5.3 Impact of attack goals

Independently of the various actors goals and motivations, these attacks will have an impact on the victim, whether the patients themselves or those other groups affected. In order to account for the various types of consequences that these attacks could have on them, we measure impact according to four separate aspects: health (H), monetary (M), privacy (P) and quality of life (QL). We chose these four factors because affecting them negatively align precisely with the attack goals we have previously discussed in Section 4.5.2. Furthermore, by separating our analysis for these factors, we aim to support different agendas and objectives of those organizations potentially interested in this kind of risk assessment, e.g. health regulation agencies, device manufacturers, health practitioners, etc. The impact scale ranges from 1 to 4, with 4 being the highest impact level (most severe). The description of the impact levels can be found in Table 4.1 and the summary of the analysis is presented in the Table 4.2. The explanation of the impact analysis by attack goal follows.

G1 (P) While confidential, the information disclosed would not have a severe consequences (except maybe in terms of insurability) and is likely to exist in other or be otherwise available to actors through other sources or other more traditional forms of cyber attacks no related to CIED. (M) The disclosure of this information may be grounds for legal action against the hospital and the manufacturer.

G2 (M) The medical device industry is very profitable, and competition between manufacturers is fierce. Losses due to intellectual property theft could reach tens of millions of dollars.

G3 (H) We consider the worst case scenario: the dependent patient (i.e. one that cannot survive without the device) for whom the doctor does not make the appropriate diagnosis potentially leading to loss of life. (M) The doctor and hospital could face severe penalties. (QL) The patient's quality of life would be affected if G3 is achieved.

G4 (H) An interruption in the patient's follow-up could have harmful effects on the patient's health, for example if an arrhythmic even occured and there is delay in initiating treatment. (M) For certain health services, time is money: the interruption of a service for a long period of time can produce losses of millions of dollars for the health organization. (QL) The patient's quality of life would be affected because of the long waits at the hospital or the increase in the number of hospital visits.

G5 (H) Worst case scenario, death of dependent patients. (M) In the event of a legal action, the company could face significant economic penalties. Moreover, the manufacturer could lose market share or have its devices removed from the market by regulators.

G6 (M) The equipment could be removed from the market, causing economic losses to the company. (QL) The patient would feel a temporary discomfort.

Table 4.2 Impact results by attacks goal

Attacks goal	**H**	**M**	**QL**	**P**
G1 Access patient sensitive data	-	1	-	2
G2 Gain knowledge of device operation and software	-	4	-	-
G3 Induce medical staff to make errors	4	3	1	-
G4 Disrupt or lower quality of patient follow-up	2	3	1	-
G5 Alter device behaviour to endanger patient	4	3	-	-
G6 Alter device behaviour to decrease quality of life	-	2	2	-

4.6 Scenario-based risk analysis

4.6.1 Vulnerabilities

We now inventory the vulnerabilities (V_i) affecting the CIED ecosystem. We have harvested this information from several sources, including ICS-CERT advisories, the NVD maintained by the NIST, the CVE database maintained by the Mitre Corporation and previous research in this area [7–9, 53]. We separated the vulnerabilities in three groups, depending on what devices they affect, with some of them applicable to more than one type of device (i.e. V_9, V_{10}). We have inventoried 15 vulnerabilities, enumerated in Table 4.3 [6], and explained in detail in the following paragraphs.

6. In this dissertation, we maintained the original names of the vulnerabilities, i.e., the technical names with which they appear on the source where we extracted them.

Table 4.3 List of vulnerabilities

	Vulnerability description
	CIED
V_1	Weak authentication algorithms
V_2	Boundless telemetry session duration
V_3	Unencrypted data storage and transmission
V_4	Lack of command whitelisting techniques
	Programmer
V_5	Unencrypted hardcoded authentication credentials
V_6	Software directory path traversal
V_7	Improper restriction of communication channel
V_8	Unprotected removable media/hard-drives
V_9	Unprotected USB serial port connections
V_{10}	Exploiting embedded debugging interfaces (JTAG and UART)
	Monitor
V_9	Unprotected USB serial port connections
V_{10}	Exploiting embedded debugging interfaces (JTAG and UART)
V_{11}	OS hardcoded authentication credentials
V_{12}	Exposed dangerous methods or functions
V_{13}	Server hardcoded authentication credentials
V_{14}	Hardcoded server parameters
V_{15}	Exploiting remote firmware update

V_1: **Weak authentication algorithms**

Certain CIED use Time-based One-time Password (TOP) for authentication. The external devices authenticate to the CIED by computing a password from the current time and a shared secret, i.e. a secret cryptographic key shared between the CIED and both the external programmer and the home-monitoring device, for certain CIED the secret key is their serial or model number. TOP authentication algorithms are vulnerable to identity theft attacks since an adversary who steals the secret key can generate valid passwords every time he wants to establish a telemetry session with the device [9, 10, 12, 50, 55].

V_2: **Boundless telemetry session duration**

The number of RF wake-up commands that a CIED can receive per session is not limited, i.e. an attacker can maintain a telemetry session indefinitely active by regularly sending the aforementioned commands to prematurely reduce the CIED's lifetime [7, 12, 51, 53].

V_3: **Unencrypted data storage and transmission**

Certain CIED models store and transmit patient information without encrypting it. Thus, a nearby attacker may intercept the data exchanged between the CIED and the programmer or even gain access to the sensitive data stored on the device by sending an unauthorized RF command [9, 12, 52, 55].

V_4: **Lack of command whitelisting techniques**

Command whitelisting is a computer protection method based on software restriction policy rules. This technique blocks by default the execution of all the programs contained in the device so that only programs that are the subject of a policy rule can be executed. In the case of CIED there are no policy rules prohibiting the execution of programming commands from devices other than external programmers. Consequently, an adversary could send a programming command to the CIED by means of commercial available equipment such as a commercially-available SDR [7, 9, 55].

V_5: **Unencrypted hardcoded authentication credentials**

The product username and password are stored in a recoverable format, i.e. without being previously encrypted [35, 36].

V_6: **Software directory path traversal**

It has been shown that the software of certain devices contain directory path traversal vulnerabilities, i.e. a kind of software implementation vulnerability that permits the access to directories other than those permitted by design. Thus, an adversary will be able to exploit these weaknesses in order to read the external programmer's file system [35, 37].

V_7: **Improper Restriction of Communication Channel**
Downloading software updates is done by means of a Virtual Private Network (VPN) established between the programmer and its software update provider. While the use of VPN is a recognized good practice to secure communications between two parties, it has been unveiled that certain external programmers models do not verify that they are still connected to the VPN before the update operation is accomplished. Thus, an adversary could leverage the device's local network access features to interfere with the communication between the programmer and its software update provider [8, 35, 38].

V_8: **Exploiting embedded debugging interfaces (JTAG and UART)**
Embedded debugging interfaces are connection ports present in a device's printed circuits. Manufacturers use them to perform functional testing and redesign of devices after manufacturing. For example, JTAG is a master/server interface used to verify a circuit, test device logic and perform functional redesign when needed. It can be used to read and modify the memory and the registers as well as to read the device's firmware. The UART interface provides a serial communication between the device's embedded systems and an external PC, i.e. a bidirectional interface used to send and receive data asynchronously. Since these interfaces allow direct access to the device memory and firmware, unprotected access to those interfaces constitutes an entry point for attacks against the CIED [8]. Home monitoring devices also have this vulnerability.

V_9: **Unprotected USB serial port connections**
Certain devices have USB port connections. They are frequently used by medical staff to store the information on a USB stick in order to transfer it to other systems, e.g. reporting software. If the USB port connection is not blocked with a password or another authentication mechanism, an attacker could connect to it and access data on the device and potentially take control of it [8].

V_{10}: **Unprotected removable media/hard-drives**
When they are in the attacker's hands, the media/hard drives become an entry point of attacks since they can be used to extract information from a device's file system [8].

V_{11}: **OS Hard coded authentication credentials**
In certain products, authentication credentials to the operating system (OS) are hard-coded on the device. That means that an adversary with physical access to the device's integrated circuit can access the OS by connecting to the debug port and authenticate with the hard-coded password [8, 39, 76].

V_{12}: **Exposed dangerous methods or functions**
Home monitors contain debug code to test their communication interfaces with both the

CIED or the external system (databases, servers) of the cloud-based application used by the physicians. Thus, by leveraging this vulnerability an adversary with physical access to the monitor can maliciously exploit the debug code to accomplish a set of attacks, for example, read or write the device's memory content, interrupt the data sending to the cloud-based systems, enable bidirectional communication with CIED [39, 40].

V_{13}: **Server hardcoded authentication credentials**
The credentials that home monitors use to authenticate to the cloud-based systems supporting the patient's remote follow-up service are hard-coded on certain devices. Thus, an attacker with physical access to the monitor can leverage these vulnerabilities to access the database in order to read or tamper with the patient's medical data [8].

V_{14}: **Server hardcoded parameters**
In certain home monitors the IP address of the authentication servers are hard-coded. An adversary could use this information to conduct a DoS attack to make the server temporarily unavailable by sending several web requests to this IP address [8].

V_{15}: **Exploiting remote firmware update**
Firmware updates for home monitors are triggered remotely. Indeed, when the time comes to update the device's firmware, the manufacturer sends the new version to the monitor through the cloud. This method is advantageous from the patient's point of view since it avoids an additional trip to the hospital. However, it constitutes at the same time an attack vector because the home-monitoring device does not verify the identity of the system distributing the firmware. An attacker could take advantage of this lack of verification by achieving a man-in-the middle attack with the purpose of sending a counterfeit firmware to the device [8].

4.6.2 Attack scenarios

Once we have identified who the actors are and what they are trying to achieve (attack goals), we are now interested in the strategy that it is going to be used by them, i.e. how will they exploit the vulnerabilities of the CIED ecosystem to achieve their goals? Thus, as illustrated in Table 4.4, an attack goal can be achieved through different scenarios. As defined in Section 4.4.2 an attack scenario is the sequence of events that must occur for the attack to take place.

It can be noticed that the same scenario can serve to achieve different attack goals. Since a threat is a pair (actor, scenario) and the actors can vary from one attack goal to the next, we carried out the scenario-based risk analysis by attack goals. The explanation of the scenarios of each attack goal follows. For a more extensive description of the sequence of events leading

to the achievement of the attack scenarios refer to B.

G1 Access patient sensitive data

There are three ways to acquire patients medical data: performing a radio attack (S_1, S_2) on the incoming RF communication between the CIED and the external devices (monitor, programmer), getting unauthorized physical access to the monitor contents (S_3) or performing a network attack on the monitor (S_4).

Executing the radio attacks described in Scenarios S_1 and S_2 requires the actor to have specialized materials and software, namely an SDR, an antenna and a radio signal processing software (e.g. GNURadio, HackRF, etc.). Once this requirement has been met, the actor must go either to the patient's home (S_1) or to the hospital(S_2), place himself at a distance relatively close to the CIED, configure its antenna in reception mode, tune it to the transmission frequency of the CIED then, record the signals emitted by the latter and read the patient's medical data by exploiting the CIED unencrypted data storage and transmission vulnerability (V_3).

The physical attack of Scenario S_3 also requires the actor to have specialized equipment. An in-debugger-circuit, a debugger IDLE and a pirate bus (or an F to F jumper wire) are needed. Since the monitor is the targeted device, the actor must go to the patient home, then connect to the device's debugging interfaces employing the pirate bus (or the F to F jumper wire). After that, he must use the in-debugger-circuit along with the debugger IDLE to access the monitor's memory content [7]. Consequently, the actor must exploit the following three vulnerabilities of the monitor: exploiting debugging interfaces (V_{10}), server hard-coded authentication credentials (V_{13}) and, hard-coded server parameters (V_{14}).

The monitor is once again the target device in Scenario S_4. Here, the network attack proposed relies on installing a backdoor on the device. In this case, the actor must know beforehand the day when an update will take place. Once done, he must approach the patient's home then, access the patient's private network, and achieve a man-in-the-middle attack exploiting the monitor's remote firmware update session (V_{15}). At that point, the actor must swap the updated firmware for a backdoor. Thus, he will be able to access the target at any later time employing the backdoor.

7. This attack scenario will be used especially when the ultimate goal of the attacker would be to subsequently attack the server to obtain the medical data of several patients.

Table 4.4 Attack scenarios

Attack goal	Scenario	Scenario description	Method
$G1$	S_1	CIED-Monitor communication interception	Intercepting RF signals with an SDR
	S_2	CIED-Programmer communication interception	Intercepting RF signals with an SDR
	S_3	Extraction of health data stored into the monitor	Connecting to the debbugging ports
	S_4	Insertion of a backdoor (malware) into the monitor	Realizing a MITM attack during a firmware update session
$G2$	S_4	Insertion of a backdoor (malware) into the monitor	Realizing a MITM attack during a firmware update session
	S_5	Extraction of the programmer's system data from the device's SW deployment network server	Sending a malicious http request to the server
	S_6	Extraction of the programmer's system data	Accessing the device through an update session's communication channel
	S_7	Reading/extraction of the monitor's files system	Accessing to the device's USB port
	S_8	Reading/extraction of the programmer's files system	Accessing to the device's USB port
	S_9	Reading/extraction of the programmer's system data	Removing the media device's hard-drive
	S_{10}	Reading/extraction of the monitor's OS information	Connecting to the debugging ports
$G3$	S_{11}	Insertion of a malware that produce programmer's reading errors	Realizing a MITM attack during an update session
	S_{12}	Introduction of calibration errors into the CIED'S microprocessor (through malware insertion or sending inappropriate commands)	Sending RF commands with an SDR
	S_{13}	Insertion of a malware that produce programmer's reading errors	Using the device's USB port
$G4$	S_4	Insertion of a ransomware (malware) into the monitor	Realizing a MITM attack during a firmware update session
	S_{11}	Insertion of a ransomware (malware) into the programmer	Realizing a MITM attack during an update session
	S_{12}	Insertion of a ransomware (malware) into the CIED	Sending RF commands with an SDR
	S_{14}	Maintain a CIED's telemetry session indefinitely open	Sending RF commands with an SDR
	S_{15}	Modify/erase the contents of the monitor memory	Connecting to the debugging ports
$G5$	S_{11}	Insertion of a malware that ignores programmers's therapy settings	Realizing a MITM attack during an update session
	S_{11}	Insertion of a malware that make programmer apply a predefined dangerous treatment	Realizing a MITM attack
	S_{11}	Insertion of a backdoor (malware) into the programmer	Realizing a MITM attack during a session update
	S_{12}	Modification of the CIED's RAM section containing the therapy's code to be applied to the patient	Sending RF unauthorized commands with an SDR
$G6$	S_{10}	Disable the periodic data transmission from the monitor	Connecting to the debugging ports
	S_{11}	Insertion of a malware that produce programmer's reading errors	Realizing a MITM attack during an update session
	S_{14}	Maintain a CIED's telemetry session indefinitely open	Sending RF commands with an SDR

G2 Gain knowledge of device operation and software

G2 can be achieved by performing network attacks on the external devices (S_4, S_6, S_7, or S_8), launching a web attack on the programmer software deployment network server (S_5), or getting unauthorized physical access to the external devices (S_9, S_{10}). In the last case we will talk about a physical attack on the external devices.

For the network attacks of Scenarios S_4, S_6, S_7, and S_8, the actor must either go to the patient's home (S_4, S_7) or the hospital (S_6, S_8). Note that for Scenarios S_4 and S_7, this must occur the day of an update of the monitor and the programmer respectively. Once on the crime scene, the actor should access either the targeted device network (S_7, S_8) or the communication channel established between the communicating parties (S_4, S_6). In the last case, the communicating parties are the external device and the web server of the entity in charge of the updates. Thus, once in the external device network the actor should either connect himself to the USB port and acquire the file system (S_7, S_8) or have direct access to the devices and therefore to the data (S_4, S_6).

In Scenario S_5 the actor must find the URL from which the programmer update application retrieve files from the server of the software deployment network. Once this is done, he modifies the URL with commands and web server escape code. After that, he sends this URL to the web server by means of a web request. Thus, if the attack is successful, the actor will be able to extract the desired files.

Getting an unauthorized physical access to the external devices (S_9 and S_{10}) is another mean to achieve G2. On Scenario S_9, the extraction of the programmer hard drive is required. Thus, the actor should go to the hospital and remove it. As far as Scenario S_{10} is concerned the attack is on the monitor, that is to say that the crime scene is the patient's home. The sequence of events of this scenario is that of S_3 except that two events are added, namely 1) connect to the debug port of the operating system and then 2) authenticate using the credentials that will have been previously acquired by performing the same actions as in S_3.

G3 Induce medical staff to make diagnostic errors

G3 can be achieved is feasible by achieving three kinds of attacks: a network attack on the programmer (S_{11}), a radio attack on the CIED (S_{12}) or a physical attacks on the programmer (S_{13}).

The sequence of events for Scenario S_{11} is practically the same as that for Scenario S_4. What differentiates both scenarios is the target device. In S_4, it is the monitor while in S_{11}, it is the programmer. Thus the only difference between S_{11} and S_4 stems from the first event,

that in the case of S_{11} is happening in the patient's home.

Scenario S_{12} is completely similar to Scenarios S_1 and S_2. The only change is the actor's behavior. Indeed, in Scenarios S_1 and S_2 he intercepts data; he is a passive actor. In Scenario S_{12}, however, he transmits data, thus he is an active actor. The events in Scenario S_{12} are otherwise practically the same events as in S_1 and S_2. We say practically because first, a new event is added. That is the transmission of data. Second, one of the events of S_1 and S_2 is modified. In fact we saw for the G1 scenario the actor would have to configure his antenna in reception mode to intercept the data, while in S_{12} it will have to put in transmission mode.

In Scenario S_{13} a network attack is performed on the programmer. The actor's purpose here is to introduce a calibration error on the device, by inserting a malware through the device's UBS port connection. In order to do so, he goes to the patient's home, accesses the patient's network, scans the network ports in order to find the one that corresponds to the USB connection, then sends the malware by means of the aforementioned port. As it can be noticed, the sequence of events for Scenario S_{13} is quite similar Scenario S_8. The difference between both is the last event which in S_8 is accessing the device file system while in S_{13} it is sending the malware.

G4 Disrupt or lower quality of patient follow-up

The goals of G4 can be accomplised by performing a network attack against the external devices (S_4, S_{11}), radio attacks against the CIED (S_{12}, S_{14}) or physical attack against the monitor. In the first cases, i.e. Scenarios S_4 and S_{11}, the purpose of the attack is to render the data of the external devices unreadable. To do this, the actor will send a ransomware to the devices, i.e. a kind of malware that encrypts the system data. Data restoration consists of applying the same operation to the encrypted data with decryption key. Normally, the malware operator will have generated and kept secret a copy of the decryption key, that will only be revealed to the victim in exchange for ransom. The sequence of the events is similar to that of S_4 and S_{11} for the G1 and G2 scenarios. The difference lies in the type of malware used, and this has no effect on the sequence of events.

For the radio attacks, the sequence of events leading to S_{12} because is similar to that in G3. What changes between the two attacks goals is the nature of the data transmitted by the actor. In G3, it is a dangerous command, here it is malware. Scenario S_{14} consists off periodically sending wake-up commands to the CIED to maintain open the incoming wireless communication. In order to do that, the actor must obtain an SDR, an antenna and a signal processing software. He must track the victim and replay an RF wake-up command every time the wireless session is about to expire.

G5 Alter device behaviour to endanger patient

G5 is achievable by perpetrating network attacks on the programmer (S_{11}). These attacks can take several forms as detailed in the Table 4.4. Indeed, the actor can implement these scenarios to send malicious code that ignores the therapy settings set by the practitioners, or introduces a calibration error into the device, or allows him to access the device by means of a backdoor. Performing a radio attack against the CIED (S_{12}) is another way to accomplish the Goal G5. The actor's purpose here will be to modify the device's RAM section containing the therapy code to be applied to the patient. As those scenarios have already been appearing in previous attacks goals scenarios (G3 and G4), the event sequence will be the same.

G6 Alter device behaviour to decrease quality of life

Three kinds of attacks can be carried out in order to achieve attack Goal G6. The first one, S_{10}, consists in perpetrating a physical attack on the monitor with the purpose of disabling the device's periodic data transmission. The second one, S_{11}, relies on the execution of a network attack on the programmer. The actor introduces a calibration error on the device by inserting malware. The third one, S_{14}, is a radio attack on the CIED. The goal will be to maintain a wireless communication session indefinitely open by sending RF wake-up commands. The event sequence is similar to that of Goal G5.

4.6.3 Probabilities of Occurrence

As defined in Section 4.4.2, the probability of occurrence (P_r) represents the chance that a given threat (actor-scenario pair) materializes. In other words, it is the likelihood that an actor achieves an attack scenario with success. By success we mean the achievement of the attack's goal or what is the same, the engendering of a specific impact on the victim. We calculate the probability by threat. That is, for each actor of each scenario. As explained in the methodology section (Section 4.4.3), P_r is calculated (3.1) as the sum of the three threat attributes: capacity (c), opportunity (o) and motivation (m). The c, o, m values vary from 1 to 4, with 4 corresponding to a higher likelihood. In the following paragraphs, we justify the rates assigned to c, o, m for each threat, with the overall P_r values given in Table 4.5.

Attack goal G1

Capacity Scenarios S_1 and S_2 are accomplished by means of radio attacks. The capacit for Actors A3 and A4 are the same ($c = 3$) for many reasons: the knowledge is abundant and accessible to all the actors, the software tools used to intercept and process RF signals are

Table 4.5 Threats probability of occurrence

Attack goal	**Scenario**	**actor**	c	o	m	P_r
$G1$	S_1	A3	3	2	2	7
		A4	3	1	1	5
	S_2	A3	3	2	2	7
		A4	3	2	1	6
	S_3	A3	2	2	2	6
		A4	1	1	1	3
	S_4	A3	3	2	2	7
		A4	3	1	1	5
$G2$	S_4	A1	4	1	2	7
		A2	3	2	4	9
		A3	3	2	3	8
		A4	3	1	3	7
	S_5	A1	4	3	2	9
		A2	4	3	4	11
		A3	4	3	3	10
		A4	3	3	3	9
	S_6	A1	4	1	2	7
		A2	3	2	4	9
		A3	3	2	3	8
		A4	3	1	3	7
	S_7	A1	4	2	2	8
		A2	3	3	4	10
		A3	3	3	3	9
		A4	3	2	3	8
	S_8	A1	4	3	2	9
		A2	3	3	4	10
		A3	3	3	3	9
		A4	3	3	3	9
	S_9	A1	4	1	1	6
		A2	4	2	1	7
		A3	4	2	1	7
		A4	4	1	1	6
	S_{10}	A1	1	1	1	3
		A2	2	2	1	5
		A3	2	2	1	5
		A4	1	1	1	3
$G3$	S_{11}	A1	4	1	1	6
		A3	3	2	3	8
		A4	3	1	3	7
	S_{12}	A1	1	1	1	3
		A3	2	2	3	7
		A4	2	1	3	6
	S_{13}	A1	4	3	1	8
		A3	3	3	3	9
		A4	3	3	3	9
$G4$	S_4	A1	3	1	1	5
		A3	2	2	3	7
		A4	2	1	2	5
	S_{11}	A1	3	1	1	5
		A3	2	2	3	7
		A4	2	1	2	5
	S_{12}	A1	3	1	1	5
		A3	2	2	3	7
		A4	2	1	2	5
	S_{14}	A1	3	1	1	5
		A3	3	2	2	7
		A4	3	1	3	6
	S_{15}	A1	1	1	1	3
		A3	3	2	3	8
		A4	2	1	2	5
$G5$	$S_{11(a)}$	A3	3	2	2	7
		A4	3	1	3	6
	$S_{11(b)}$	A3	2	2	2	6
		A4	1	1	3	5
	$S_{11(c)}$	A3	3	2	2	7
		A4	3	1	3	7
	S_{12}	A3	2	2	2	6
		A4	2	1	3	6
$G6$	S_{10}	A1	1	1	1	3
		A3	2	2	3	7
		A4	1	1	3	5
	S_{11}	A1	4	1	1	6
		A3	3	2	3	8
		A4	3	1	3	7
	S_{14}	A1	3	1	1	5
		A3	3	2	3	8
		A4	3	1	3	6

increasingly simpler to use, thus reducing the attack's technical difficulty, and the equipment needed to perform these attacks (SDR and antenna) is not expensive. For Scenario S_3, even if the knowledge is accessible to all the actors and the equipment needed to conduct the attack is not expensive, the attack is technically complex to achieve. Indeed, it involves the exploitation of two vulnerabilities for which solid knowledge of computer programming and architecture is required. Normally, Actor A3 recruits experts with exceptional technical skills and have more human resources. They have more capacity than Actor A4. Thus, in Scenario S_3 A3 capacity ($c = 2$) is higher than the one of Actor A4 ($c = 1$). Scenario S_4 is a network attack and thus additional material is not required. Additionally, there is nowadays extensive information available and tools to perform the attack in S_4 . Thus, capacity for Actors A3 and A4 will be the same ($c = 3$) in this scenario.

Opportunity In Scenarios S_1 and S_3, the attack takes place in the patient's home. In these cases Actor A3 ($o = 2$) has a better chance than Actor A4 ($o = 1$) since they are specifically trained to infiltrate private sites without being noticed. In Scenario S_2, the attack takes place in the hospital during a patient's medical visit. The latter implies that adversaries only have approximately two days a year to conduct the attack, coinciding with the number of times patients go to the doctor. However, since hospitals are public places, the actors are less likely to be noticed. Thus, the opportunity score for Actors A3 and A4 ($o = 2$) is the same. In Scenario S_4 the attacks take place during a monitor's update session, which takes place only about once a year. Actor A3 access to this information and opportunity to leverage it is greater ($o = 2$) than that of Actor A4 ($o = 1$).

Motivation Both Actors A3 and A4 benefit from the crime. They gain access to sensitive personal information. For A3, this attack objective is in line with the *raison d'être* of their profession, i.e. obtaining private information from individuals. Thus the motivation of Actor A3 ($m = 2$) will be higher than that of Actor A4 (m =1) because for A3 this attack objective is an end in itself while for A4 it is a means to an end (sow national disorder).

Attack goal G2

Capacity In Scenario S_5 a web attack is launched. There is information and tools available online to perform this kind of attack. Actor type A4 are experts in the field (web attack). On the other hand, Actors A2 and A3 are specialists in the extraction of information from people or systems. In addition, they often have specialized human resources. Thus the capacity of A1, A2 and A3 ($c = 4$) is the same and it is higher than that of A4 ($c = 3$). In Scenarios S_4,

S_6, S_7 and S_8 network attacks are conducted. Once more, information and tools are available to achieve these attacks. However, because they have more know-how than the others on the matter (i.e. network attacks) Actor A4's capacity ($c = 4$) is higher than that of A1, A2 and A3 ($c = 3$). The attack performed in S_9 has no major technical complications. It is necessary to remove a hard disk and then mount it later in another computer media. Thus, the capacity of all actors will be the same ($c = 4$). However, the achievement of Scenario S_{10} presents a major challenge. On the one hand, solid technical knowledge of computer programming and architecture is necessary. In addition, there is no extensive information about how to realize the exploit in S_{10} . Thus, Actors A2 and A4's capacity ($c = 2$) is higher than that of A1 and A4 ($c = 1$) since A2 and A3 normally are experts with exceptional technical skills and have more human resources.

Opportunity Scenario S_5 is a web attack where there is no restriction of time and space. So the actors' opportunity will be higher and the same ($o = 3$). Scenarios S_6 and S_4 take place during targeted device update sessions, during which there are constraints in terms of time (update session) and space (near the patient's home or hospital). As far as the time constraint is concerned, Actors A2 and A3 have better possibilities to know when an update session will take place. In terms of space constraint, A2 and A3 have the same opportunities either at the patient's home or in the hospital. However, A1 and A4 will have more chances in the hospital as this is a public place where they can go unnoticed. Thus on the S_6 and S_4 Scenarios, Actors A2 and A3 opportunity is higher ($o = 2$) than that of A1 and A4 ($o = 1$). For Scenarios S_7, S_8, S_9 and S_{10} there is no time constraint but there is still a space constraint. Scenarios S_7 and S_8 require the actor to be near either the patient's home or the hospital in order to access their network, whereas for S_9 and S_{10} the actor must to have physical access to the targeted devices. Similarly as for S_7, since the attack takes place near to patient's home Actors A2 and A3 opportunity ($o = 3$) will be higher than the one of Actors A1 and A4 ($o = 2$). For S_8 however, all actors opportunity score is the same ($o = 3$) since the attack takes place in a public site. In Scenarios S_9 and S_{10}, since the attack requires physical access to the device Actors A2 and A3 opportunity ($o = 2$) is higher tan that of A1 and A4 ($o = 1$).

Motivation All actors benefit from the crime. They gain system information. A2 motivation ($m = 4$) is the highest since the goal of this attack is the purpose of their profession. Actors A3 and A4 follow them with the same level of motivation ($m = 3$). The motivation of A1 (m=2) is the lowest because obtaining system information is not an end but a means to accomplish their activities.

Attack goal G3

Capacity Attack scenarios S_{11}, S_{12} and S_{13} consist in introducing reading or calibration errors on the CIED's ecosystems devices. To do that knowledge of the device inner workings and advanced programming skills are required. Since there is some but not a lot of available information about how programmers and monitors work, in Scenarios S_{11} and S_{13} the capacity of A1 ($c = 4$) will be higher than that of A3 and A4 ($c = 3$). The reason is that A1 are experts in the development of malicious code. On the other hand, there is much less information available about CIED and their architecture. Thus, for Scenario S_{12}, the capacity of the actors will be the same ($c = 2$). This is due to the fact that while A1 are experts in malware development, A3 and A4 are more likely to obtain the CIED's mode of operation either by hiring personnel skilled in CIED programming or by using other illegal methods.

Opportunity For Scenarios S_{11} and S_{12} there are constraints in terms of time and space. Scenario S_{11} takes place in the hospital during a session update. Scenario S_{12} must be performed near the patient and during an incoming wireless communication with one of the externals devices. In these scenarios, we apply the same opportunity values that we have applied to the scenarios S_6 and S_4. That is to say that in S_{11} and S_{12}, Actor A3's opportunity ($o = 2$) is higher than that of Actors A1 and A4 ($o = 1$). On S_{13} there is only a space restriction, and the same reasoning as in Scenario S_8 is applied: all actors have the same opportunity ($o = 3$).

Motivation Actors A1, A3 and A4 all benefit from the attack. Actor A1 conducts these attacks in order to make money, whereas Actors A3 and A4 are motivated by the opportunity to cause harm. Thus, Actors A3 and A4's motivation is the same ($m = 3$) and higher than that of Actor A1 ($m = 1$) since for the latter there are other ways to make more money faster.

Attack goal G4

Capacity In Scenario S_{14} a replay attack is performed. There is no major challenge in conducting this attack, which consists in periodically transmitting a Wake-Up command to the CIED by means of an SDR. Thus Actors A1, A3 and A4's capacity is the same ($c = 3$). However, in Scenarios S_{12}, S_{11} and S_4, Actor A1's capacity is higher ($c = 3$) than that of A3 and A4 ($c = 2$), since these scenarios consist in implanting a ransomware, and A1 are experts on malicious code development. For Scenario S_{15} advanced knowledge in computer programming and architecture is needed. Thus, Actor A3's capacity ($c = 3$) will be higher

because they have more human resources and specialized personnel, followed by, Actors A4 ($c = 2$) and A1 ($c = 1$).

Opportunity In Scenarios S_{14} and S_{12} there are still constraints in terms of time and space. The actor must be close to the patient in order to send radio commands with its antenna to the CIED . Moreover, the attack must take place while the wireless communication is established in the CIED. As in the other scenarios where these constraints are presents, the opportunity of Actor A3 ($o = 2$) is always higher than that of Actors A1 and A4 ($o = 1$). In Scenarios S_4 and S_{11}, the situation is the same, the actor being limited by space (home or hospital) and time (update sessions). Normally, when there is only a space constraint all actors have the same opportunity at the hospital (S_{11}) because it is a public place and, while Actor A3 has more opportunity at home (S_4). However, since in Scenario S_{11} there is the additional the time constraint that it happens during an update session, the actors opportunity will be the same in both scenarios. Thus, in Scenarios S_{11} and S_4 the opportunity of A3 ($o = 2$) is higher than that of A1 and A4 ($o = 1$). In Scenario S_{15}, physical access to the targeted system, i.e. the monitor, is required. Thus, the opportunity for Actor A3 ($o = 2$) is higher than that of A1 and A4 ($o = 1$).

Motivation Actors A1, A3 and A4 all benefit from the attack. By performing these attack scenarios, A3 ($m = 2$) and A4 ($m = 3$) would succeed in endangering patients' lives and consequently harming their quality of life, while A1 ($m = 1$) would make money through ransom.

Attack goal G5

Capacity Since there is extensive information about the external programmer behaviour, the capacity of Actors A3 and A4 ($c = 3$) is the same on Scenarios $S_{11(a)}$ and $S_{11(c)}$. For Scenario $S_{11(b)}$ knowledge of Cardiology is required, and Actor A3 is more likely to have access to personnel with such knowlegde or hiring it. Thus, A3's capacity ($c = 2$) is higher than that of A4 ($c = 1$). On Scenario S_{12}, the capacity of the Actors A3 and A4 will be the same ($c = 2$). The reasoning is the same as that for Scenario S_{12} (Section 4.6.3), namely the lack of information concerning the CIED's behaviour and implementation.

Opportunity The analyis of the opportunity factor for Scenario S_{14} (Section 4.6.3) apply equally to Scenario S_{12}. Thus, the opportunity of A3 ($o = 2$) is higher than that of A4 ($o = 1$). The same is true for the analysis of opportunity for Scenario S_{11} on Attack Goal G3

(Section 4.6.3), which applies to Scenarios $S_{11(a)}$, $S_{11(b)}$ and $S_{11(c)}$. That is to say that the opportunity of A3 ($o = 2$) is higher than that of A4 ($o = 1$).

Motivation This attack goal clearly aims at harming the health of an individual. Thus it is Actor A3 ($m = 2$) and Actor A4 ($m = 3$) that benefit most from this attack. We do not give them maximum motivation because there are many faster and equally subtle ways to achieve this goal.

Attack goal G6

For Scenario S_{10} the analysis made in Section 4.6.3 in terms of capacity and opportunity equally applies. For Scenarios S_{11} and S_{14}, the capacity and opportunity socres are the same as those of Section 4.6.3 and 4.6.3,n respectively. In terms of motivation the same reasoning than for Attack Goal G3 (4.6.3) is applied.

4.6.4 Combined risk assessment

Risk assessment values range between 3 and 48. They are calculated as the probability (ranging from 3 to 12) multiplied by the impact (from 1 to 4). We calculate the risk separately for each impact category. This way of doing things gives insight of the risk that each threat (scenario, actor) represents separately for the health, economy, quality of life and privacy impact categories. Consequently, this analysis responds to the needs of several different groups such as medical practitioners, regulators, manufacturers and even patients. Each will know what the riskiest threat is for him and therefore the one to treat with priority. We ranked the risks in Table 4.6. Depending on the risk value, different risk management strategies can be chosen and applied. There are four strategies for managing risk, namely *refuse*, *accept*, *transfer* or *manage* the risk. The most drastic is of course to refuse the risk, which is when the risk is considered unacceptable because of the catastrophic consequences it may have on the victims. In those cases, it is recommended to prohibit, stop using or remove the system posing the threat. The strategy of accepting the risk is applied when the risk is either negligible or acceptable. That is to say when the benefits that the system bring outweigh its potential risks. Transfering the risk relies on giving the risk management responsibility to a third party such as an insurance company. This is a strategy that is not really applicable in those threats where the impact is on patient health or quality of life. Finally, the risk mitigation or risk management strategy consists in reducing the risk as much as possible with available means. This can be done through the updates of the systems, stricter regulations or even awareness campaigns.

Table 4.6 Risk characterization

Risk level	Values	Management strategy
– Unacceptable	R=[36,48]	Refuse
– Undesirable	R=[24,35]	Manage
– Acceptable	R=[12,23]	Accept
– Negligeable	R=[3,11]	Accept

4.7 Results and Discussion

The attacks goals of inducing medical staff to make errors (G3) and alter device behavior to endanger patient (G5) represent a risk for patient health. Those to gain knowledge of device operation and software (G2), induce medical staff to make errors (G3) and disrupt or lower quality of patient follow-up (G4) represent an economic risk to manufacturers and health organizations. We can then note that G3 represents a risk for all groups. In terms of privacy or degradation of life quality, none of the attack goals represent a potential risk that needs to be managed. In this section, we focus on those threats representing either an unacceptable or an undesirable risk for the victims' health and economy. The risk results of all the threats herein considered can be found in Table 4.6 of the appendix A.

4.7.1 Monetary risk assessment

Monetary risk assessment by attack goals

Attack goal G2 This attack goal represents a major risk in terms of economic losses. The victim can be either the manufacturer or the hospital. As hospitals are public organization, it can be considered that it is the whole society that is the victim. G2 contains five unacceptable threats (Scenarios S_4, S_5, S_6, S_7 and S_8 with all actors). These threats should be managed with high priority. By analyzing these threats, we can see that the actor's attack method is always the same, namely exploiting the authentication mechanisms of the target systems, i.e. the external devices and cloud-based systems with which they interact. This fact in itself is good news. On the one hand, external devices are not constrained by the resource limitations as the CIED are, so robust authentication solutions can be implemented without significant problems. There is a plethora of standard robust and proven solutions to secure system authentication, and there is no need to resort to proprietary, unproven solutions. We, therefore, propose the following solutions.

The threats related to Scenario S_4 are solved by securing domestic networks. To do this, patients must take the habit of securing their network with a robust password, e.g. a password

containing upper and lower case characters, numbers and special characters. This password should be periodically changed. Also, the patient should pay attention to the other Internet of Things (IOT) devices that are connected to his network, as they can be the entry door to their network. Accordingly, they should ensure that all devices in their networks are secured with a password.

To solve the threats associated with Scenario S_5, it is essential to insist that web developers use good code practices and that the source code of web pages be periodically reviewed.

To mitigate the threats associated with Scenario S_6, hospitals and manufacturers should adopt more reliable VPN solutions even if they require more investment. Besides, hospitals and manufacturers should consider recruiting cybersecurity professionals and technical services whose responsibility will be to ensure that there are no cybersecurity threats in their systems and/or networks, including those used for CIED programming and management.

For the threats associated with Scenarios S_7 and S_8, the solution involves securing USB ports of monitors and programmers with robust passwords, which should be continuously modified.

The threat posed by Scenario S_9 is not as significant. This means that it must be managed. The solution is simple: physical security of the targets devices, in this case, programmers. In addition, it would be necessary to carry out awareness campaigns among the staff who use those devices, so that they become aware of the scope of the problem and therefore more attentive to the physical security of these devices.

Attack goal G3 The threats associated with the scenarios S_{11} and S_{13} represent an undesirable risk. In order to mitigate the first threat, hospitals and manufacturers should adopt more reliable VPN solutions. The mitigation of the second threat involves securing the USB ports of the programmers with robust passwords.

Attack goal G4 The threat related to Scenario S_{10} represents an undesirable risk whose mitigation is to protect the debugging interface ports with a password.

Monetary risk assessment by attack vectors

From an economic point of view, the vulnerabilities V_6, V_7, V_9, and V_{15} must be eliminated, because their exploitation constitutes an unacceptable risk for the hospitals and the manufacturers. V_6 is eliminated by using good programming practices and revising the source code of the programmers' software. V_7 by securing hospital networks, and adopting more reliable VPN solutions. The security of hospital networks can also be improved by implementing

Table 4.7 Results of the monetary risk assessment

Risk level	Management strategy
– Unacceptable	Refuse
– Undesirable	Manage
– Acceptable	Accept
– Negligeable	Accept

Attack goal	Scenario	Attack vector	P_{rMax}	I	R
G_1 Access patients sensitive data	S_1	3	7	1	7
	S_2	3	7	1	7
	S_3	10,13,14	6	1	6
	S_4	15	7	1	7
G_2 Gain Knowledge of device operation and software	S_4	15	9	4	36
	S_5	6	11	4	44
	S_6	7	9	4	36
	S_7	9	10	4	40
	S_8	9	10	4	40
	S_9	8	7	4	28
	S_{10}	10,11,12	5	4	20
G_3 Induce medical staff to make errors	S_{11}	7	8	3	24
	S_{12}	1,4,5	7	3	21
	S_{13}	9	9	3	27
G_4 Disrupt or lower quality of patient follow-up	S_4	15	7	3	21
	S_{11}	7	7	3	21
	S_{12}	1,4,5	7	3	21
	S_{14}	2	7	3	21
	S_{15}	10	8	3	24
G_5 Alter device behavior to endanger patient	$S_{11(a)}$	7	7	3	21
	$S_{11(b)}$	7	6	3	18
	$S_{11(c)}$	7	7	3	21
	S_{12}	1,4,5	6	3	18
G_6 Alter device behavior to decrease quality of life	S_{10}	10,11,12	7	2	14
	S_{11}	7	8	2	16
	S_{14}	2	8	2	16

efficient identity and access management (IAM) rules. For V_9, it is necessary to secure the USB ports of the external devices with strong passwords. Finally, securing home networks with strong passwords would eliminate the vulnerability V_{15}. Once the vulnerabilities mentioned above have been addressed, vulnerability V_8 must be managed as a priority because its exploitation constitutes an undesirable risk for hospitals. To do that, they must ensure the physical security of the programmer devices.

4.7.2 Health risk assessment

Health risk assessment by attack goals

Attack goal G3 The results of Table 4.8 reveal that G3 is the riskiest attack goal in terms of health. This is because of the unacceptable risk that Scenario S_{13} represents, i.e. the insertion of malware on the programmer through a USB port connection aimed to generate reading errors. Among the riskiest threats of this attack goal, this one must be managed with priority. However, the solution is simple: protect USB port connection with a robust password and frequently change this password. During our observation of operations in a pacemaker clinic, we observed that it is common practice for staff to record the readings of the programmer (during follow-up sessions) in a USB key and then insert the key into a medical report formatting software in a separate computer system. We recommend that staff pay attention because this USB key could be the target of the actors. They could install the malware on it, and it would infect the programmer. Secondly, the computer where the software is located could also be the target of the actor. This means that the actor could infect the computer, subsequently the computer would infect the USB key, and then the programmer. Thus, it is necessary to pay attention to who is using the USB key, and then to ensure that the computer containing the report formatting software is itself secure (e.g. not connected to the network, unless strictly necessary).

The threats related to Attack Scenarios S_{11} and S_{12} constitute an undesirable risk that need to be mitigated. For Scenario S_{11}, the threat consists in the insertion of malware into the programmer. S_{11} is achievable by accessing the device network during the programmer update session. The threat, as mentioned above, is avoidable by securing the health center network. Accordingly, it is necessary to implement an efficient method of identity and access management (IAM) of the computer systems of those entities. On the other hand, S_{12} threat takes advantage of the improper restriction of communication channels during the programmer updates. As mentioned in Section 4.6.1, those updates are achieved through a VPN between the device and the entity in charge of the updates. Thus, the health centers and manufacturers must invest in reliable solutions of VPN. For Scenario S_{12}, the threat is the

insertion of malware on the CIED. This threat is due to the lack of robustness of the CIED authentication mechanisms. One potentital solution consists in implementing more robust authentication mechanisms by using well-known techniques (e.g. asymmetric cryptography). However, CIED are limited in terms of computing resources and such solutions are not the most appropriate. There are, however, other more adequate solutions, which could be applied during the CIED manufacturing process. In particular, we propose that manufacturers use whitelisting techniques in the CIED software, which would prevent devices other than the programmer from sending commands to the CIED.

Attack goal G5 As in Attack Goal G3, the achievement of Scenarios S_{11} and S_{12} constitutes undesirable risk that must be managed. The same recommendations made for G3 therefore also apply here.

Health risk assessment by attack vectors

From a health point of view, vulnerability V_9 must be eliminated because its exploitation represents an unacceptable risk to the health of individuals. This is feasible by securing the USB ports of the external devices with strong passwords. Once V_9 is adequately managed, Vulnerabilities V_6, V_7 and V_5 must be managed as a priority because their exploitation constitutes an undesirable risk. To mitigate the risk that V_6 represents, good programming practices and code source revision must take place on the programmer software. To reduce the risk associated with V_7, the hospital networks must be secured, and reliable VPN solutions must be applied. Finally, to mitigate V_5 it is necessary to apply whitelisting techniques on the CIED.

4.8 Conclusion

As evidenced by previous work, CIED are vulnerable to cyber attacks that use their RF interfaces to communicate with external devices (programmer and home monitor). This fact has been proven by the realization of radio attacks against the CIED RF communication interface in research laboratories [7, 9]. Additionally, the telemetry functionality of the externals devices introduces vectors of cyber attacks [8]. Those can include manipulation of the home monitor, interception of transmissions from the home monitor to the cloud and the physician's station, and manipulation of the cloud-based database itself. Although the vulnerabilities mentioned above exist, no attacks have been reported until now in real life, i.e. in an environment other than the controlled environment of research laboratories.

Table 4.8 Results of the health risk assessment

Risk level	Management strategy
– Unacceptable	Refuse
– Undesirable	Manage
– Acceptable	Accept
– Negligeable	Accept

Attack goal	Scenario	Attack vector	P_{rMax}	I	R
G_3 Induce medical staff to make errors	S_{11}	7	8	4	32
	S_{12}	1,4,5	7	4	28
	S_{13}	9	9	4	36
G_4 Disrupt or lower quality of patient follow-up	S_4	15	7	2	14
	S_{11}	7	7	2	14
	S_{12}	1,4,5	7	2	14
	S_{14}	2	7	2	14
	S_{15}	10	8	2	16
G_5 Alter device behavior to endanger patient	$S_{11(a)}$	7	7	4	28
	$S_{11(b)}$	7	6	4	24
	$S_{11(c)}$	7	7	4	28
	S_{12}	1,4,5	6	4	24

Thus, it remained to be determined how viable such an attack would be on an actual target (person or device) in the real world. This led us to the following research question: What are the real risks of cyber attacks onto CIED and the systems they depend on (programmer, monitor, cloud-based systems)? To answer this question, we carried out a realistic risk analysis of such attacks, with regards to their impact at four scales: health, economy, quality of life and privacy. We proceeded in this way because the problem under study affects many different groups namely: patients, practitioners, manufacturers, and more broadly states. Accordingly, separating the scales aims to individually support those groups objectives in terms of risk management.

We did three kinds of analysis. First, an actor-based risk analysis to determine who the actors are and what their attack goals are. This analysis allowed us to determine the level of impact of the attacks. We then made a scenario-based risk analysis to determine the probability of occurrence of the attacks. Finally, we performed a combined risk analysis by considering the impact and probability results. We determined the most dangerous attack goals on the one hand, and the most dangerous vulnerabilities on the other.

Our work reveals that the vulnerabilities associated with the RF communication interface of CIED represents an acceptable risk. This is due to the fact that these vulnerabilities have a low probability of being successfully exploited in real conditions (environment other than

a research laboratory). However, the network and Internet connectivity of external devices represents a risk that in some cases is unacceptable, i.e. a risk that must be absolutely refused. The answer to our research question is therefore that the real risk is in the external devices and not in the CIED and that this risk is due to the increasing connectivity of said devices. We can therefore see that the problem under study is the medical variant of the trendy cyber-security problem: the lack of security of connected objects (Internet of Thing or IOT).

Indeed, among the 15 vulnerabilities identified, four constitute an unacceptable risk. They are V_6, V_7, V_9, and V_{15} and are all to external devices. Five other vulnerabilities (V_1, V_4, V_5, V_8, andV_{10}) represent an undesirable risk, i.e. a risk that must be addressed. Among the latter two are vulnerabilities specific to CIED (V_1,V_4). However, their exploitation will have an impact if and only if another specific programmer vulnerability is successfully exploited (V_5). There are already existing solutions to avoid all those vulnerabilities. The parties involved have to put them into practice. In order to achieve this, stronger regulation and legislation is needed. These should not be limited to good practice guidelines without any force of law as is the case today. In the same manner, the FDA or Health Canada (or other similar national organizations) should impose that hardware components of medical equipment pass a set of certification tests including cyber security assessment in order to be accepted in the market; the same should be the case for their software components. Finally, the various involved parties (practionners, patients, etc.) should be duly informed of the origin, nature and scope of the threats and how to protect themselves at their level. This information must be disclosed in language that is understandable to them so that they can take part in the solution.

Moreover, our analysis revealed that the attack goals (G2) *Gain knowledge of device operation and software* and (G3) *Induce medical staff to make errors* are the main attack goals of the actors. This result shows that while attacks on these devices affect patients, the patients are not always the target as we may have thought so far. The targets in many cases are manufacturers (intellectual property theft) and practitioners (threat of civil liability) for purely economic reasons. Manufacturers should, therefore, be aware of the problem and focus on the computer security of their equipment. The first step to this is avoiding secrecy regarding the software and architecture of their equipment. As has been often posited, code is more secure when it is open source since several people can test it and report errors so that they can be patched. This secrecy about code instead of protecting manufacturers, exposes them more to cyber security risk. Health centers have to become more selective and demanding with the equipment they buy and implant on patients, as this would allow them to put more pressure on manufacturers to make the right cyber security choices.

CHAPITRE 5 DISCUSSION GÉNÉRALE

Les DECI sont vulnérables aux attaques informatiques qui exploitent leurs interfaces de communication RF. De plus, les fonctionnalités de télémétrie et de connectivité IP des systèmes externes dont ils dépendent introduisent de nouveaux vecteurs d'attaque. Par conséquent, l'écosystème en étude connaît un accroissement des facteurs de risque reliés aux attaques informatiques.

Bien qu'il existe de nos jours des solutions pour éviter les attaques informatiques contre les technologies de l'information et de la communication. Notamment les méthodes cryptographiques ou le hachage cryptographique. Ces méthodes traditionnelles de la sécurité informatique ne peuvent être directement appliquées aux DECI en raison des limitations de ressources (énergie, microprocesseur, mémoire) qu'ils présentent.

Par ailleurs, bien que les systèmes externes dont les DECI dépendent ne soient contraints en matière de ressources, les mesures de sécurité qui y sont implémentées ne sont pas les adéquates à cause du manque d'information régnant. En effet, nous avons constaté en réalisant ce travail qu'il existe une surabondance d'information au sujet des vulnérabilités qui affectent ces systèmes. Cependant cette information est technique, par conséquent elle n'est pas toujours compréhensible pour la majorité des parties affectées (patients, médecins). Outre cela, ladite information ne met pas en lumière les scénarios d'attaque (où, quand, comment) où est-ce que les vulnérabilités pourraient être exploitées. Une telle démarche permettrait non seulement de sensibiliser les parties affectées, mais aussi de les induire à prendre les mesures de sécurité idoines pour se protéger.

Afin de réduire le risque d'attaques informatiques dans l'écosystème des DECI, il est nécessaire que les parties affectées d'une part connaissent les menaces (acteur, scénarios). D'autre part il faut qu'elles sachent la portée du risque pour adresser les menaces les plus risquées en priorité. Dans l'intention de combler ce besoin, notre objectif de recherche a été de déterminer la portée réelle du risque (aux attaques informatiques) encouru par les éléments de l'écosystème des DECI. Ainsi, nous avons formulé la question de recherche suivante *Quel est le risque d'exploitation réelle des vecteurs d'attaque (vulnérabilités) affectant l'écosystème des DECI ?*

En vue de répondre à cette question de recherche, une analyse du risque de cybersécurité encourue par l'écosystème des DECI a été réalisée. Pour ce faire, trois objectifs spécifiques ont été fixés: 1) déterminer l'impact des attaques contre l'écosystème des DECI, 2) estimer la probabilité d'occurrence des menaces, 3) caractériser le risque des-dites menaces. Ainsi, par

le moyen de cette analyse de risque nous apportons trois contributions. Premièrement, nous déterminons la portée réelle du risque encouru par les dispositifs en étude. Deuxièmement, nous identifions les menaces qui doivent être adressées en priorité. Troisièmement, nous fournissons des recommandations sur la manière d'adresser ces menaces.

Pour atteindre le premier objectif spécifique i.e. déterminer l'impact des attaques, une analyse de risque basé sur les acteurs a été réalisée. Les résultats de cette analyse révèlent que les attaques informatiques contre l'écosystème des DECI ont un impact non seulement sur la santé du patient, mais aussi un impact économique sur les bénéfices des fabricants et les coûts des hôpitaux. Notre analyse démontre que l'impact que ce type d'attaque peut avoir sur la qualité de vie des patients ou sur la confidentialité de leurs informations personnelles est bas. À travers notre analyse, nous constatons que lorsque l'acteur veut avoir un impact sur la santé, ses objectifs d'attaque sont soit inciter le personnel médical à faire des erreurs (G3), soit modifier le comportement des dispositifs (G5). Lorsque l'acteur veut avoir un impact économique sur les bénéfices des fabricants ou les coûts des centres hospitaliers, ses objectifs d'attaque seront acquérir des connaissances sur le fonctionnement des appareils et logiciels (G2), inciter le personnel médical à faire des erreurs (G3) ou encore, perturber la qualité du suivi du patient (G4).

La deuxième partie de la recherche a consisté à élaborer une analyse de risques basé sur les scénarios d'attaques. Avec cette analyse, nous avons atteint le deuxième objectif spécifique de cette recherche i.e. estimer la probabilité d'occurrence des menaces. Les résultats de cette partie révèlent que les menaces ayant le plus de probabilité d'occurrence sont des attaques web (scénario S_5) ou des attaques réseau contre les dispositifs externes (scénarios S_7 et S_8). Par ailleurs, les résultats de notre travail démontrent aussi que les attaques radio qui exploitent l'interface de communication RF des DECI ont une probabilité d'occurrence moyenne voire basse tout dépendamment du scénario d'attaque. Bien que ces attaques soient simples à réaliser du point de vue technique, cela n'en est pas de même du point de vue pratique. Les résultats de nos expériences au laboratoire et de notre analyse de risque basé sur les scénarios d'attaque illustrent ce fait. Nous observons que les opportunités dont dispose l'acteur pour matérialiser les menaces sont limitées en raison des contraintes de temps et d'espace que présentent les attaques radio contre les DECI. D'une part, les menaces ne peuvent se matérialiser qu'au cours d'une session de communication sans fil entre le DECI et l'un des dispositifs externes (programmeur et moniteur). Cette contrainte de temps limite l'opportunité de l'acteur à cinq minutes par jour si la session de communication exploitée a lieu entre le DECI et le moniteur. Par contre, si la session de communication exploitée a lieu entre le DECI et le programmeur son opportunité se réduit à quelques minutes lors des visites à l'hôpital. D'autre part, ce type d'attaque ne peut avoir lieu que chez le patient

ou à la salle de consultation des DECI à l'hôpital. Cette contrainte d'espace vient limiter davantage les opportunités de l'acteur du fait que les chances qu'il a de se faire remarquer sont élevées.

Finalement, pour atteindre le troisième objectif spécifique (caractériser le risque des menaces) et par conséquent répondre à notre question de recherche, nous avons réalisé une analyse de risque combinée. Celle-ci est dite combinée car elle se sert des résultats de l'analyse du risque basée sur les acteurs et l'analyse du risque basée sur les scénarios d'attaque pour fournir le risque associé aux menaces qui affectent l'écosystème des DECI. Le risque a été calculé en fonction des résultats d'impact et de probabilité d'occurrence. L'analyse de risque combinée révèle d'une part que les menaces les plus risquées correspondent aux systèmes externes et non pas aux DECI. D'autre part, que ces menaces se matérialisent soit par des attaques réseau soit par des attaques web. Par conséquent, les résultats obtenus dans l'analyse de risque combinée donnent réponse à la question de recherche. À savoir que, les vulnérabilités qui encourent un risque réel d'exploitation appartiennent aux dispositifs externes, et que le risque d'exploitation de l'interface de communication RF des DECIS est acceptable. Par conséquent, les vulnérabilités inacceptables ou indésirables des systèmes externes dont dépendent les DECI doivent être adressées en priorité. Tandis que les vulnérabilités liées à l'interface de communication RF des DECIS ne nécessitent pas de mesures de gestion immédiates du fait que leur risque d'exploitation est acceptable. Notre analyse du risque basée sur les scénarios d'attaque démontre que la solution passe par la sécurisation des réseaux où sont déployés les éléments de l'écosystème des DECI et, par la sécurisation des services médicaux dans le nuage. De plus, bien que l'interface de communication RF des DECI constitue une menace, le risque encouru est acceptable et ne nécessite pas de mesures de gestion immédiates.

Pour conclure, ce travail met en évidence que cela n'est pas prioritaire d'investir en sécurité informatique pour les DECI eux-mêmes. En revanche, un renforcement de la sécurité des systèmes externes dont dépendent les DECI, des réseaux dans lesquels ces systèmes sont déployés ainsi que des services médicaux basés dans le nuage qui dépendent de ces systèmes externes, s'avère primordial et prioritaire.

CHAPITRE 6 CONCLUSION

6.1 Limitations de nos travaux

Les vulnérabilités que nous avons analysées dans ce travail datent du début de l'étude. Vers la fin de nos travaux, une nouvelle vulnérabilité nommée *BleedingBit* [88] a été dévoilée, elle affecte les dispositifs ayant des puces Bluetooth comme les DECI ou les pompes à insuline. Cette vulnérabilité permet à un attaquant de prendre le contrôle intégral des périphériques vulnérables sans s'authentifier. La vulnérabilité exploite une faiblesse de la logique du protocole BLE (Bluetooth Low Energy) utilisée dans ces appareils. À notre connaissance celle-ci est la seule vulnérabilité parue depuis le début de notre étude mais il pourrait y en avoir d'autres qui n'ont pas encore été dévoilées au grand public. Par conséquent, nos résultats d'analyse du risque par vecteurs d'attaque pourraient ne plus correspondre à la situation actuelle du fait que "BleedingBit" ou d'autres vulnérabilités non publiées pourrait avoir plus de criticité que les vulnérabilités que nous avons considérées.

Nous avons réalisé en laboratoire des attaques radios contre un modèle de DECI et de programmeur dans le but d'évaluer les chances de succès des dites attaques. Ainsi, bien que ces expérimentations nous aient aidés à estimer la probabilité d'occurrence de ce type attaques, celle-ci (la probabilité d'occurrence) serait plus précise si nous avions réalisé les expérimentations sur des modèles (DECI et programmeur) d'autres fabricants. Cependant nous ne disposions pas de tels modèles. De plus, bien que nous disposions de moniteurs, nous n'avons pas pu faire des attaques radio contre eux. Lorsqu'un moniteur est assigné à un patient, le fabricant " hard-code" les crédentielles d'authentification (le numéro de série) du DECI sur le moniteur. Ainsi, un moniteur ne communique qu'avec un seul DECI. Bien évidemment, il existe un moyen pour ce faire avec ces crédentielles d'authentification. Il faudrait démonter le moniteur, extraire son circuit intégré et se connecter aux interfaces UART ou JTAG pour avoir accès au contenu de la mémoire et par conséquent, acquérir les crédentielles d'authentification souhaités. Cependant, nous n'étions pas autorisés à démonter les moniteurs pour raisons de confidentialité.

Dans notre analyse basée sur les acteurs nous n'avons pas considéré les acteurs accidentels. C'est à dire les personnes qui pourraient être une source de menace par négligence ou par inadvertance. En les considérant nous aurions déterminé plus de menaces (acteur, scénario) et cela nous aurai permis de leur donner des recommandations pour éviter le risque.

6.2 Recherches futures

En vue des limitations de notre travail, nous proposons deux améliorations. D'une part, que le risque des nouvelles vulnérabilités publiées qui n'ont pas été considérées dans cette étude faute de temps devraientt être évalué. D'autre part, les sources de risque accidentelles devrait être considérées dans l'analyse de risque basée sur les scénario d'attaque. En effectuant ces améliorations, la prévision de la portée du risque serait plus précise et par conséquent plus en concordance avec la réalité.

Suite aux résultats obtenues dans ce travail de recherche a savoir que, investir en sécurité informatique dans les DECI n'est pas prioritaire et que le risque réel d'attaques informatiques se trouve dans les réseaux et les services de santé basées dans le nuage, nous proposons d'une part que les recherches futures généralisent ce travail à d'autres dispositifs médicaux implantables comme les pompes à insuline, les implant cochléaires ou encore les implants cérébraux (*BrainChips*). Nous suggérons d'autre part qu'une analyse du risque des infrastructures médicales en général soit réalisée; par infrastructures médicales, nous entendons l'ensemble des TIC présentes dans les centres hospitaliers et qui sont accessibles par réseau ou connectivité IP.

RÉFÉRENCES

[1] Institut de Cardiologie de Montréal. (2014) Installation d'un stimulateur cardiaque (pacemaker). [En ligne]. Disponible:https://www.icm-mhi.org/fr/soins-et-services/examens-et-traitements/installation-dun-stimulateur-cardiaque-pacemaker

[2] World Society of Arythmias. (2018) How many people have pacemakers. [En ligne]. Disponible:https://www.reference.com/health/many-people-pacemakers-ad932529c8ba04dd

[3] Statistica. (2016) Global number of pacemakers in 2016 and a forecast for 2023 (in million units)*. [En ligne]. Disponible:https://www.statista.com/statistics/800794/pacemakers-market-volume-in-units-worldwide/

[4] E. Cuvillier, *Handbook of Leads for Pacing, Defibrillation and Cardiac Resynchronization.* Cardiotext, 2011.

[5] H. S. Savci, A. Sula, Z. Wang, N. S. Dogan et E. Arvas, "Mics transceivers: regulatory standards and applications [medical implant communications service]," dans *Southeastcon, 2005. Proceedings. IEEE.* IEEE, 2005, p. 179–182.

[6] R. S. Sanders et M. T. Lee, "Implantable pacemakers," *Proceedings of the IEEE*, vol. 84, n°. 3, p. 480–486, 1996.

[7] E. Marin, D. Singelée, F. D. Garcia, T. Chothia, R. Willems et B. Preneel, "On the (in) security of the latest generation implantable cardiac defibrillators and how to secure them," dans *Proceedings of the 32nd Annual Conference on Computer Security Applications.* ACM, 2016, p. 226–236.

[8] B. Rios et J. Butts, "Security evaluation of the implantable cardiac device ecosystem architecture and implementation interdependencies," 2017.

[9] D. Halperin, T. S. Heydt-Benjamin, B. Ransford, S. S. Clark, B. Defend, W. Morgan, K. Fu, T. Kohno et W. H. Maisel, "Pacemakers and implantable cardiac defibrillators: Software radio attacks and zero-power defenses," dans *IEEE Symposium on Security and Privacy (SP).* IEEE, 2008, p. 129–142.

[10] Barnaby Jack. (2012) Pacemaker hack can deliver deadly 830-volt joltl. [En ligne]. Disponible:http://white-hackers.blogspot.com/2012/10/pacemaker-hack-can-deliver-deadly-830.html

[11] Food and Drug Administration. (2017) Firmware update to address cybersecurity vulnerabilities identified in abbott's (formerly st. jude medical's) implantable

cardiac pacemakers: Fda safety communication. [En ligne]. Disponible:https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm573669.htm

[12] ICS-CERT. (2017) Advisory icsma-17-241-01. [En ligne]. Disponible:https://ics-cert.us-cert.gov/advisories/ICSMA-17-241-01

[13] Radcliffe, Benjamin. (2011) Hacking medical devices for fun and insulin: Breaking the human SCADA system. [En ligne]. Disponible:https://www.youtube.com/watch?v=-q29b3wvbss

[14] A. Burns, M. E. Johnson et P. Honeyman, "A brief chronology of medical device security," *Communications of the ACM*, vol. 59, n°. 10, p. 66–72, 2016.

[15] e-monsite. (2013) Comment corriger les bradycardies par le biais du pacemake. [En ligne]. Disponible:http://pacemaker-tpe.e-monsite.com/pages/ii-un-moyen-de-remedier-a-cette-anomalie-le-pacemaker/1-qu-est-ce-qu-un-pacemaker.html

[16] Washington Heart Rhythm Associates, LLC. (2015) Implantable cardioverter defibrillator (icd). [En ligne]. Disponible:http://www.washingtonhra.com/pacemakers-icds/implantable-cardioverter-defibrillator-icd.php

[17] C. F. Holmes, "Lithium/halogen batteries," dans *Batteries for Implantable Biomedical Devices*. Springer, 1986, p. 133–180.

[18] R. W. Baker, "Pacemaker programmer with telemetric functions," U.S Brevet U.S. 4 550 370 A, 29 oct. 1991. [En ligne]. Disponible:https://patents.google.com/patent/US4550370A/

[19] J. A. Sholder et B. Mann, "Programmable automatic implantable cardioverter/defibrillator and pacemaker system," U.S Brevet U.S. 4 989 602 A, 5 feb. 1991. [En ligne]. Disponible:https://patents.google.com/patent/US4989602A/

[20] B. P. Brockway, R. D. Dreher, D. E. Huntwork, B. S. Lindstedt, D. C. Morrison et P. A. Mills, "Programmable multi-mode cardiac pacemaker," U.S Brevet U.S. 4 562 841 A, 25 sep. 1990. [En ligne]. Disponible:https://patents.google.com/patent/US4562841A/

[21] S. R. Duggan, "Adaptable, digital computer controlled cardiac pacemaker," U.S Brevet U.S. 4 958 632 A, 25 sep. 1990. [En ligne]. Disponible:https://patents.google.com/patent/US4958632A/

[22] C. H. A. Segerstad, A. Lekholm et H. Elmqvist, "Pacemaker architecture: A pacemaker with an attached computer or a computer with an attached pacemaker," *Pacing and Clinical Electrophysiology*, vol. 7, n°. 6, p. 1213–1216, 1984.

[23] A. Bernstein et V. Parsonnet, "Microcomputer and microprocessor applications in cardiac pacing." *Medical instrumentation*, vol. 17, n°. 5, p. 329–333, 1983.

[24] Medtronic. Medtronic carelink 2090 reference manual programmer for medtronic and vitatron devices. [En ligne]. Disponible:https://www.manualslib.com/manual/1410977/Medtronic-Carelink-2090.html#manual

[25] Biotronik USA. Eluna HF-T technical manual. [En ligne]. Disponible:https://manualzz.com/doc/7597543/eluna-hf-t---biotronik-usa

[26] Medscape Internal Medicine , LLC. (2002) New pacemakers, icds with home monitoring save time. [En ligne]. Disponible:https://www.medscape.org/viewarticle/433442

[27] R. P. Ricci, L. Morichelli, A. D'onofrio, L. Calò, D. Vaccari, G. Zanotto, A. Curnis, G. Buja, N. Rovai et A. Gargaro, "Effectiveness of remote monitoring of cieds in detection and treatment of clinical and device-related cardiovascular events in daily practice: the homeguide registry," *Europace*, vol. 15, n°. 7, p. 970–977, 2013.

[28] D. Slotwiner, N. Varma, J. G. Akar, G. Annas, M. Beardsall, R. I. Fogel, N. O. Galizio, T. V. Glotzer, R. A. Leahy, C. J. Love *et al.*, "Hrs expert consensus statement on remote interrogation and monitoring for cardiovascular implantable electronic devices," *Heart Rhythm*, vol. 12, n°. 7, p. e69–e100, 2015.

[29] K. Jeffrey et V. Parsonnet, "Cardiac pacing, 1960–1985: a quarter century of medical and industrial innovation," *Circulation*, vol. 97, n°. 19, p. 1978–1991, 1998.

[30] T. Mittal, "Pacemakers—a journey through the years," *Indian Journal of Thoracic and Cardiovascular Surgery*, vol. 21, n°. 3, p. 236–249, 2005.

[31] A. J. Salkind et S. Ruben, "Mercury batteries for pacemakers and other implantable devices," dans *Batteries for implantable biomedical devices*. Springer, 1986, p. 261–274.

[32] J. Drews, G. Fehrmann, R. Staub et R. Wolf, "Primary batteries for implantable pacemakers and defibrillators," *Journal of power sources*, vol. 97, p. 747–749, 2001.

[33] A. J. Salkind, A. J. Spotnitz, B. V. Berkovits, B. B. Owens, K. B. Stokes et M. Bilitch, "Electrically driven implantable prostheses," dans *Batteries for Implantable Biomedical Devices*. Springer, 1986, p. 1–36.

[34] L. Stotts, "Vlsi applications in implantable medical electronics," dans *Electron Devices Meeting, 1989. IEDM'89. Technical Digest., International*. IEEE, 1989, p. 9–14.

[35] ICS-CERT. (2018) Advisory ICSMA-18-058-01. [En ligne]. Disponible:https://ics-cert.us-cert.gov/advisories/ICSMA-18-058-01

[36] NIST. (2018) NVD-CVE-2018-5446 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-5446

[37] NIST. (2018) NVD-CVE-2018-5448 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-5448

[38] NIST. (2018) NVD-CVE-2018-10596 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-10596

[39] ICS-CERT. (2018) Advisory ICSMA-18-179-01. [En ligne]. Disponible:https://ics-cert.us-cert.gov/advisories/ICSMA-18-179-01

[40] NIST. (2018) NVD-CVE-2018-8868 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-8868

[41] N. R. Potlapally, S. Ravi, A. Raghunathan et N. K. Jha, "Analyzing the energy consumption of security protocols," dans *Proceedings of the 2003 international symposium on Low power electronics and design*. ACM, 2003, p. 30–35.

[42] C. Camara, P. Peris-Lopez et J. E. Tapiador, "Security and privacy issues in implantable medical devices: A comprehensive survey," *Journal of biomedical informatics*, vol. 55, p. 272–289, 2015.

[43] H. Rathore, A. Mohamed, A. Al-Ali, X. Du et M. Guizani, "A review of security challenges, attacks and resolutions for wireless medical devices," dans *Wireless Communications and Mobile Computing Conference (IWCMC), 2017 13th International*. IEEE, 2017, p. 1495–1501.

[44] M. Rostami, A. Juels et F. Koushanfar, "Heart-to-heart (h2h): authentication for implanted medical devices," dans *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*. ACM, 2013, p. 1099–1112.

[45] G. Zheng, G. Fang, R. Shankaran, M. A. Orgun et E. Dutkiewicz, "An ecg-based secret data sharing scheme supporting emergency treatment of implantable medical devices," dans *Wireless Personal Multimedia Communications (WPMC), 2014 International Symposium on*. IEEE, 2014, p. 624–628.

[46] X. Hei et X. Du, "Biometric-based two-level secure access control for implantable medical devices during emergencies," dans *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, p. 346–350.

[47] K. B. Rasmussen, C. Castelluccia, T. S. Heydt-Benjamin et S. Capkun, "Proximity-based access control for implantable medical devices," dans *Proceedings of the 16th ACM conference on Computer and communications security*. ACM, 2009, p. 410–419.

[48] F. Xu, Z. Qin, C. C. Tan, B. Wang et Q. Li, "Imdguard: Securing implantable medical devices with the external wearable guardian," dans *INFOCOM, 2011 Proceedings IEEE*. IEEE, 2011, p. 1862–1870.

[49] T. A. Nesheim, "The ble cloaker: Securing implantable medical device communication over bluetooth low energy links," thèse de doctorat, California

Polytechnic State University, San Luis Obispo, San Luis Obispo, CA, 2015. [En ligne]. Disponible:https://digitalcommons.calpoly.edu/cgi/viewcontent.cgi?referer=&httpsredir=1&article=2621&context=theses

[50] NIST. (2017) NVD-CVE-2017-12712 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2017-12712

[51] NIST. (2017) NVD-CVE-2017-12714 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2017-12714

[52] NIST. (2017) NVD-CVE-2017-12716 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2017-12716

[53] X. Hei, X. Du, J. Wu et F. Hu, "Defending resource depletion attacks on implantable medical devices," dans *Global telecommunications conference (GLOBECOM 2010), 2010 IEEE*. IEEE, 2010, p. 1–5.

[54] C. Li, A. Raghunathan et N. K. Jha, "Hijacking an insulin pump: Security attacks and defenses for a diabetes therapy system," dans *e-Health Networking Applications and Services (Healthcom), 2011 13th IEEE International Conference on*. IEEE, 2011, p. 150–156.

[55] Ruxon. (2012) Breakpoint 2012. [En ligne]. Disponible:http://2012.ruxconbreakpoint.com/

[56] S. Jagannathan et A. Sorini, "A cybersecurity risk analysis methodology for medical devices," dans *2015 IEEE Symposium on Product Compliance Engineering (ISPCE)*, May 2015, p. 1–6.

[57] I. Stine, M. Rice, S. Dunlap et J. Pecarina, "A cyber risk scoring system for medical devices," *International Journal of Critical Infrastructure Protection*, vol. 19, p. 32–46, 2017.

[58] M. Howard et S. Lipner, *The security development lifecycle*. Microsoft Press Redmond, 2006, vol. 8.

[59] L. Kohnfelder et P. Garg, "The threats to our products," *Microsoft Interface, Microsoft Corporation*, 1999.

[60] H. Abrar, S. J. Hussain, J. Chaudhry, K. Saleem, M. A. Orgun, J. Al-Muhtadi et C. Valli, "Risk analysis of cloud sourcing in healthcare and public health industry," *IEEE Access*, vol. 6, p. 19 140–19 150, 2018.

[61] C. J. Alberts et A. Dorofee, *Managing information security risks: the OCTAVE approach*. Addison-Wesley Longman Publishing Co., Inc., 2002.

[62] D. L. Hayes, P. J. Wang, D. W. Reynolds, N. M. Estes, J. L. Griffith, R. A. Steffens, G. L. Carlo, G. K. Findlay et C. M. Johnson, "Interference with cardiac pacemakers by cellular telephones," *New England Journal of Medicine*, vol. 336, n°. 21, p. 1473–1479, 1997.

[63] Eric Blossom. (2001) Gnu radio - the free & open source radio ecosystem · gnu radio. [En ligne]. Disponible:https://www.gnuradio.org/

[64] Johannes Pohl. (2016) Github - jopohl/urh: Universal radio hacker: investigate wireless ... [En ligne]. Disponible:https://github.com/jopohl/urh

[65] M. N. Islam et M. R. Yuce, "Review of medical implant communication system (mics) band and network," *ICT Express*, vol. 2, n°. 4, p. 188–194, 2016.

[66] F. C. Commission *et al.*, "Medical implant communications service (mics) federal register," *Rules Reg*, vol. 64, n°. 240, p. 69 926–69 934, 1999.

[67] F. Rules, "Regulations," *MICS Band Plan," Table of Frequency Allocations, Part*, vol. 95, 2003.

[68] R. Bashirullah, "Wireless implants," *IEEE microwave magazine*, vol. 11, n°. 7, p. S14–S23, 2010.

[69] T. J. Cox, "Frequency agile telemetry system for implantable medical device," U.S Brevet U.S. 6 763 269 B2, 13 jul. 2004. [En ligne]. Disponible:https://patents.google.com/patent/US6763269B2/

[70] S. Hanna, "Regulations and standards for wireless medical applications," dans *International Symposium on Medical Information and Communication Technology*, 2009, p. 23–26.

[71] T. ABC. (2005) Listen before talk LBC. [En ligne]. Disponible:http://www.telecomabc.com/l/lbt.html

[72] T. ABC. (2005) AFA. [En ligne]. Disponible:http://www.telecomabc.com/a/afa.html

[73] D. B. Kramer, M. Baker, B. Ransford, A. Molina-Markham, Q. Stewart, K. Fu et M. R. Reynolds, "Security and privacy qualities of medical devices: an analysis of fda postmarket surveillance," *PLoS One*, vol. 7, n°. 7, p. e40200, 2012.

[74] F. Bastani et T. Tang, "Improving security of wireless communication in medical devices," *Massachusetts Institute of Technology*, 2015.

[75] Piggin Richard. (2017) Cyber threat source descriptions. [En ligne]. Disponible:https://www.bsigroup.com/en-GB/medical-devices/resources/whitepapers/Cybersecurity_of_medical_devices/

[76] NIST. (2018) NVD-CVE-2018-8870 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-8870

[77] ICS-CERT. (2005) Cyber threat source descriptions. [En ligne]. Disponible:https://ics-cert.us-cert.gov/content/cyber-threat-source-descriptions#gao

[78] Cyberpolicy. (2017) Why medical records are 10 times more valuable than credit card info. [En ligne]. Disponible:https://cyberpolicy.com/cybersecurity-education/why-medical-records-are-10-times-more-valuable-than-credit-card-info

[79] Aatif Sulleyman. (2017) Nhs cyber attack: why stolen medical information is so much more valuable than finantial data. [En ligne]. Disponible:https://www.independent.co.uk/life-style/gadgets-and-tech/news/nhs-cyber-attack-medical-data-records-stolen-why-so-valuable/-to-sell-financial-a7733171.html

[80] Robert Lord. (2017) The real threat of identity theft is in your medical records, not credit cards. [En ligne]. Disponible:https://www.forbes.com/sites/forbestechcouncil/2017/12/15/the-real-threat-of-identity-theft-is-in-your-medical-records-not-credit-cards/#12b202291b59

[81] Mariya Yao. (2017) Your electronic medical records could be worth $ 1000 to hackers. [En ligne]. Disponible:https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-to-hackers/

[82] Lucintel. (2018) Medical device market report: Trends, forecast and competitive analysis. [En ligne]. Disponible:https://www.businesswire.com/news/home/20180423006381/en/Global-Medical-Device-Market-Report-2018-2023-Trends

[83] K. D. Lind, "Understanding the market for implantable medical devices," *Insight*, 2017.

[84] A. Halligan, "The importance of values in healthcare," *Journal of the Royal Society of Medicine*, vol. 101, n°. 10, p. 480–481, 2008.

[85] D. Pilgrim, F. Tomasini et I. Vassilev, *Examining trust in healthcare: A multidisciplinary perspective*. Macmillan International Higher Education, 2010.

[86] E. Van der Schee, P. P. Groenewegen et R. D. Friele, "Public trust in health care: a performance indicator?" *Journal of Health Organization and Management*, vol. 20, n°. 5, p. 468–476, 2006.

[87] P. de Zulueta, "Truth, trust and the doctor–patient relationship," dans *Primary Care Ethics*. CRC Press, 2018, p. 1–24.

[88] NIST. (2018) NVD-CVE-2018-16986 detail. [En ligne]. Disponible:https://nvd.nist.gov/vuln/detail/CVE-2018-16986

ANNEXE A RISK ASSESSMENT RESULTS BY ATTACK GOALS AND IMPACT TYPE

Table A.1 Risk assessment results

Risk level	Management strategy
– Unacceptable	Refuse
– Undesirable	Manage
– Acceptable	Accept
– Negligeable	Accept

Impact type	
Health	H
Monetary	M
Life Quality	LQ
Privacy	P

				H		M		LQ		P	
Attack goal	Scenario	Attack vector	P_{rMax}	I	R	I	R	I	R	I	R
$G1$ Access patient sensitive data	S_1	3	7	-	-	1	7	-	-	2	14
	S_2	3	7	-	-	1	7	-	-	2	14
	S_3	10,13,14	6	-	-	1	6	-	-	2	12
	S_4	15	7	-	-	1	7	-	-	2	14
$G2$ Gain knowledge of device operation and software	S_4	15	9	-	-	4	36	-	-	-	-
	S_5	6	11	-	-	4	44	-	-	-	-
	S_6	7	9	-	-	4	36	-	-	-	-
	S_7	9	10	-	-	4	40	-	-	-	-
	S_8	9	10	-	-	4	40	-	-	-	-
	S_9	8	7	-	-	4	28	-	-	-	-
	S_{10}	10,11,12	5	-	-	4	20	-	-	-	-
$G3$ Induce medical staff to make errors	S_{11}	7	8	4	32	3	24	1	8	-	-
	S_{12}	1,4,5	7	4	28	3	21	1	7	-	-
	S_{13}	9	9	4	36	3	27	1	9	-	-
$G4$ Disrupt or lower quality of patient follow-up	S_4	15	7	2	14	3	21	1	7	-	-
	S_{11}	7	7	2	14	3	21	1	7	-	-
	S_{12}	1,4,5	7	2	14	3	21	1	7	-	-
	S_{14}	2	7	2	14	3	21	1	7	-	-
	S_{15}	10	8	2	16	3	24	1	8	-	-
$G5$ Alter device behaviour to endanger patient	$S_{11(a)}$	7	7	4	28	3	21	-	-	-	-
	$S_{11(b)}$	7	6	4	24	3	18	-	-	-	-
	$S_{11(c)}$	7	7	4	28	3	21	-	-	-	-
	S_{12}	1,4,5	6	4	24	3	18	-	-	-	-
$G6$ Alter device behaviour to decrease quality of life	S_{10}	10,11,12	7	-	-	2	14	2	14	-	-
	S_{11}	7	8	-	-	2	16	2	16	-	-
	S_{14}	2	8	-	-	2	16	2	16	-	-

ANNEXE B SEQUENCE OF EVENTS OF THE ATTACK SCENARIOS

S_1 : Radio attack on the CIED-Programmer wireless communications.
(e_1)Acquire the hardware (SDR, antenna, signal processing software)
(e_2)Go to the hospital
(e_3)Be located at a distance relatively close to the CIED
(e_4)Configure the SDR in reception mode
(e_5) Perform a frequency scan of the MICS band to determine the transmission frequency of the CIED
(e_6) Intercept and record the signal transmitted by the CIED
(e_7)Read the patient's health data (V_3)

S_2 : Radio attack on the CIED-Monitor wireless communications.
(e_1)Acquire the hardware (SDR, antenna, signal processing software).
(e_2)Go to the patient's home
(e_3)Be located at a distance relatively close to the CIED
(e_4)Configure the SDR in reception mode
(e_5) Perform a frequency scan of the MICS band to determine the transmission frequency of the CIED
(e_6)Intercept and record the signal transmitted by the CIED
(e_7) Read the patient's health data (V_3)

S_3: Unauthorized physical access to the monitor content
——————Using the JTAG interface——————
(e_1)Acquire the hardware (F to F jumper wire, in-debugger-circuits, PC with IDLE debugger)
(e_1)Go to the patient's home
(e_2)Take the patient's monitor
(e_3)Connect one extremity of the F to F jumper wire to the monitor debug port (exploiting V_{10})
(e_4)Connect the other extremity of the F to F jumper wire to the in-debugger-circuits
(e_5)Connect the in-debugger-circuit to the PC
(e_6)Access the monitor memory by means of the IDLE debugger
(e_7)Use V_{13} and V_{14} to adjust the server settings and credentials to authenticate to them

(e_8)Access the server by means of the information obtained in (e_8)
(e_9)Read the patient's medical data

————————Using the UART interface————————
(e_1)Acquire the hardware (Pirate bus, PC with IDLE debugger)
(e_2)Go to the patient's home
(e_3)Take the patient's monitor
(e_4)Connect one end of the pirate bus to the monitor debug port (exploiting V_{10})
(e_5)Connect the other pirate bus end to the PC containing the IDLE debugger
(e_6)Access the monitor memory by means of the IDLE debugger
(e_7)Use V_{13} and V_{14} to adjust the server settings and credentials to authenticate to them
(e_8)Access the server by means of the information obtained in (e_7)
(e_9)Read the patient's medical data

S_4 : Network attack on the Monitor
(e_1)Gain access to the patient's router the day of the monitor's update
(e_2)Intercept the updated firmware (V_{15})
(e_3)Replace the firmware with a backdoor

S_5: Web attack on programmers' SW deployment network server
(e_1)Find the URL in which the programmer (app) retrieve files from the server
(e_2)Modify URL with commands and web server escape code
(e_3)Send the URL to the server(via http request) (e_3)
(e_4)Extract the desired files

S_6 :Network attack on the programmer's
(e_1)Go to the hospital the day of the update
(e_2)Access the programmer's network
(e_3)Leverage V_7 to gain access to the programmer
(e_3)Extract the desired files

S_7: Network attack on the Monitor
(e_1)Go to the patient home
(e_2)Acces the patient network
(e_3)Acces the monitor's USB port (V_9)

(e_4)Navigate in the file system and extract the desired files

S_8: Network attack on the Programmer
(e_1)Go to the hospital
(e_2)Acces the hospital network
(e_3)Acces the monitor's USB port (V_9)
(e_4)Navigate the file system and extract the desired files

S_9: Physical attack on the Programmer
(e_1)Go to the hospital
(e_2)Extract the programmer's removable hard drive(V_8)

S_{10}: Physical attack on the monitor
————————Using the JTAG interface————————
(e_1)Acquire the hardware (F to F jumper wire, in-debugger-circuits, PC with IDLEs debugger)
(e_2)Go to the patient's home
(e_3)Take the patient's monitor
(e_4)Connect one end of the F to F jumper wire to the monitor debug port (V_{10})
(e_5)Connect the other end of the F to F jumper wire to the in-debugger-circuits
(e_6)Connect the in-debugger-circuit to the PC
(e_7)Access the monitor memory by means of the IDLE debugger
(e_8)Use V_{11} and V_{12} to adquer the credentials of OS
(e_9)Access the OS of the monitor by means of the information obtained in e_8
(e_{10})Read the OS
————————Using the UART interface————————
(e_1)Acquire the hardware (Pirate bus, PC with IDLE debugger)
(e_2)Go to the patient's home
(e_3)Take the patient's monitor
(e_4)Connect one end of the pirate bus to the monitor debug port (V10)
(e_5)Connect the other pirate bus end to the PC containing the IDLE debugger.
(e_6)Access the monitor memory by means of the IDLE debugger
(e_7)Use V_{11} and V_{12} to acquire the credentials of the OS
(e_8)Access the OS of the monitor by means of the information obtained in e_7
(e_9)Read information about OS

S_{11}: Network attack on the programmer
(e_1)Gain access to the pacemakers room consultation the day of the update
(e_2)Intercept the updated firmware (V_7)
(e_3)Replacing the firmware with malware

S_{12}: Radio attack on the CIED
(e_1)Acquire the hardware (SDR, antenna, signal processing software)
(e_2)Go to the hospital
(e_3)Be located at a distance relatively close to the CIED
(e_4)Configure the SDR in Transmission mode
(e_5) Perform a frequency scan of the MICS band to determine the Programmer's transmission frequency
(e_6) Transmit commands (via RF signals) to the CIED (V_1,V_4,V_5)

S_{13}: Network attack on the programmer
(e_1)Go to the hospital
(e_2)Access the hospital network
(e_3)Access the monitor's USB port(V_9)
(e_4)Insert a malware

S_{14}: Radio attack on the CIED
(e_1)Acquire the hardware (SDR, antenna, signal processing software)
(e_2)Go to the hospital
(e_3)Be located at a distance relatively close to the CIED
(e_4)Configure the SDR in Transmission mode
(e_5) Perform a frequency scan of the MICS band to determine the Programmer's transmission frequency
(e_6) Transmit Wake-up commands (via RF signals) to the CIED periodically (V_1,V_2,V_4)